

# GlobalSec

Cybersecurity Magazine | April 2024 | Issue 04

## FORECASTING THE STORM: THE FUTURE OF CYBER THREAT INTELLIGENCE

### *The* **CISO's VOICE**

Exclusive Interview  
with **Mr. Yigal Akerman**,  
CISO at DataLoop

**THE RESILIENT ENTERPRISE:**  
ALIGNING CYBERSECURITY  
WITH BUSINESS CONTINUITY  
GOALS

**PRIVACY BY DESIGN:**  
**BUILDING SECURITY**  
**INTO THE DIGITAL**  
**BLUEPRINT**

# Welcome



FROM THE  
EDITOR

Welcome to our 4th edition of GlobalSec magazine, the forefront of digital defense, where we explore the latest in cybersecurity innovations and insights to safeguard your digital data.

Under the **CISO's Corner**, the first article ([Page 6](#)), highlights the importance of tabletop exercises in cybersecurity, demonstrating how simulated cyber-attacks can significantly enhance an organization's incident preparedness and response strategies. The second article ([Page 8](#)), examines the pivotal role of CISO's in guiding and leading their organizations through cyber crises, focusing on effective incident response strategies.

In our monthly interview with a CISO, you can enjoy our interview with Mr. Yigal Akerman, the CISO of DataLoop ([Page 12](#)).

Under the **CISO's Buyer's Guide** ([Page 14](#)), you can gain some insight into the world of cybersecurity threat intelligence, and what you need to know before purchasing these services.

Under the **Compliance Corner** ([Page 18](#)), you'll find a great article on how to develop a framework for setting information security objectives.

Under the **Privacy Corner** ([Page 22](#)), the article explores the concept of "Privacy by Design", advocating for the integration of robust security measures right from the initial stages of digital product and system development.

Under the **Career Corner** ([Page 26](#)), the article outlines the essential skills and knowledge required to break into the cybersecurity field, preparing readers for the demands of this critical industry in the digital age.

Under the **Cyber Resilience Corner** ([Page 28](#)), the article discusses integrating cybersecurity with business continuity planning, emphasizing the creation of resilient enterprises that can withstand and recover from cyber incidents.

Under the **Features corner** ([Page 30](#)), the first article provides a roadmap for navigating the complex cybersecurity landscape of 2024, highlighting key trends, challenges, and solutions that businesses need to be aware of in the digital age.

**Our cover story** ([Page 34](#)) delves into the future of cyber threat intelligence, forecasting how evolving technologies and shifting threat landscapes will shape our cybersecurity strategies.

Under the **Technical Corner** ([Page 36](#)), you can read and learn about a useful method for conducting a risk assessment in industrial control systems and OT networks.

Under our **Experts Views corner**, the first expert view ([Page 40](#)) explores the dual-edge AI in cybersecurity, assessing whether its capabilities serve as a safeguard or pose new risks within digital security landscapes. Our second expert view ([Page 41](#)) examines the impact of GDPR and subsequent regulations on cybersecurity strategies, highlighting how compliance requirements are driving organizations to revamp their data protection measures.

In this month's edition of our Cybersecurity Library Project (CSLP), as usual, our experts recommend two more books for your exploration ([Page 42](#)).

Enjoy our monthly edition of GlobalSec magazine, and I would love to hear your thoughts.

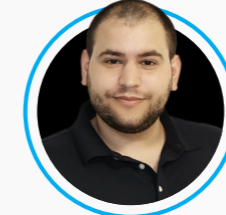
## Danny Abramovich, Editor in Chief

# CONTRIBUTORS



**OR LEVI**  
Co-Founder of  
Simplycert

The Digital Frontier:  
Navigating the Cybersecurity  
Landscape in 2024 ([30](#))



**ALEN HERSHKO**  
Security Architect at  
Global-e, and Ex-CISO

Cybersecurity Threat  
Intelligence Services: What  
Do You Need to Know? ([14](#))



**DANIEL MIKHAILOV**  
Team Leader at Titans  
Security Group

Privacy by Design: Building  
Security into the Digital  
Blueprint ([22](#))



**SHMAYA TEXON**  
Business Continuity  
Manager at Discount Bank

The Resilient Enterprise: Aligning  
Cybersecurity with Business  
Continuity Goals ([28](#))



**SHAHAR AVENSTEIN**  
CISO at SAM  
Seamless Networks

Forecasting the Storm:  
The Future of Cyber Threat  
Intelligence ([34](#))



**BELLA SILONI**  
GRC Specialist  
at SimplyCert

Breaking into Cybersecurity:  
Skills you need for the  
digital ages ([26](#))



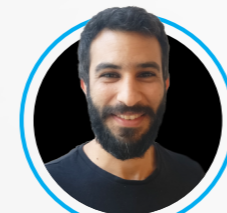
**YIGAL AKERMAN**  
CISO  
at DataLoop

Exclusive Interview with  
Mr. Yigal Akerman, CISO  
at DataLoop ([12](#))



**GIL OHAYON**  
CISO  
at Artist

GDPR and Beyond: How  
compliance is shaping  
cybersecurity strategies? ([41](#))



**EREZ LEVI**  
CISO  
at Lusha

Cyber Crisis Leadership:  
The Role of CISOs in  
Incident Response ([8](#))



**YOSI SHAVIT**  
CISO and Head of ICS  
Cyber Security Dept.

Risk Assessment in Industrial  
Control Systems and OT  
Networks that control  
hazardous materials ([36](#))



**MONAS SHMUEL**  
CISO at Local  
Government

AI in Cybersecurity: Savior  
or Threat? ([40](#))



**SAPIR COHEN**  
GRC Manager at Titans  
Security Group

Demystifying the ISO 27001:2022  
Requirements: Developing a  
Framework for Setting Information  
Security Objectives ([18](#))

### LIABILITY

While much attention and care were devoted to preparing this magazine, the publishers cannot be held responsible for the accuracy of the information or any consequences arising from it. TS-Media takes no responsibility for the content of external websites whose addresses are published in the magazine. Additionally, the views expressed within the scope of this magazine are not necessarily those of the Editor or the Publisher. TS-Media and Titans Security Group Ltd. accept no third-party products and services liability.

### COPYRIGHT

©TS-MEDIA © All rights reserved. TS-MEDIA is a trading name of Titans Security Group Ltd. In whole or in part, publication of the text included is forbidden unless the publishers grant permission in writing. Note to contributors: All materials (i.e., articles, letters, emails, faxes, photographs, drawings, etc.) submitted for consideration by the Editor must be the original work of the author and not previously published.

Pictures included, which are not the property of the contributor, were reproduced with obtained permission from the copyright owner. The Editor cannot guarantee a personal response to all letters and emails received. © Copyright Titans Security Ltd.

### DISCLAIMER

All brand or product names are trademarks of their respective owners. Please get in touch with us if we have not granted credit to your copyright. Our company ensures the correction of any oversights.

### EDITORIAL

**Editor in Chief**  
Danny Abramovich  
**Senior Editor**  
Shlomi Mordechai  
**Reviews Editor**  
Or Levi

### Contributing Editor

Alen Hershko  
**News Editor**  
Daniel Mikhailov

### ADVERTISING

**Group Advertising Manager**  
Orit Abramovich  
orit@titans2.com  
+972-77-5150340  
**Production Editor**  
Nikol Huri

### MANAGEMENT

**Managing Director**  
Danny Abramovich  
**Group Advertising Director**  
Orit Abramovich  
**Chief Executive**  
Or Levi

### CONTACT US

**Email us!**  
info@titans2.com  
**Call us!**  
+972-77-5150340

# CONTENTS

## CISO'S Corner

### Page 6 - Tabletop Exercises: Simulating Cyber Attacks to Enhance Incident Preparedness

Demonstrate how simulated cyber-attacks enhance incident preparedness

### Page 8 - Cyber Crisis Leadership: The Role of CISOs in Incident Response

Examine the pivotal role of CISO's in guiding a cyber crisis

## THE CISO'S BUYER GUIDE Corner

### Page 14 - Cybersecurity Threat Intelligence Services: What Do You Need to Know?

What do you need to know before you purchase cyber threats intelligence services

## COMPLIANCE Corner


### Page 18 - Demystifying the ISO 27001:2022 Requirements: Developing a Framework for Setting Information Security Objectives

Learn how to develop a framework for setting security objectives

## PRIVACY Corner

### Page 22 - Privacy by Design: Building Security into the Digital Blueprint

Implement PbD by building security into the digital blueprint



## THE CISO'S VOICE

Page 12 - Exclusive Interview with **Mr. Yigal Akerman**, CISO at DataLoop

## CAREER Corner

### Page 26 - Breaking into Cybersecurity: Skills you need for the digital age

What are the essential skills and knowledge to break into cybersecurity field

## CYBER RESILIENCE Corner

### Page 28 - The Resilient Enterprise: Aligning Cybersecurity with Business Continuity Goals

Integrate cybersecurity with Business continuity services

## FEATURES Corner

### Page 30 - The Digital Frontier: Navigating the Cybersecurity Landscape in 2024

Highlight key trends, challenges and solutions to combat cyber threats in 2024

### Page 34 - Forecasting the Storm: The Future of Cyber Threat Intelligence

Learn how evolving technologies will shape the future of cybersecurity



## TECHNICAL Corner

### Page 36 - Risk Assessment in Industrial Control Systems and OT Networks that control hazardous materials

Learn how to conduct a risk assessment for ICS and OT networks

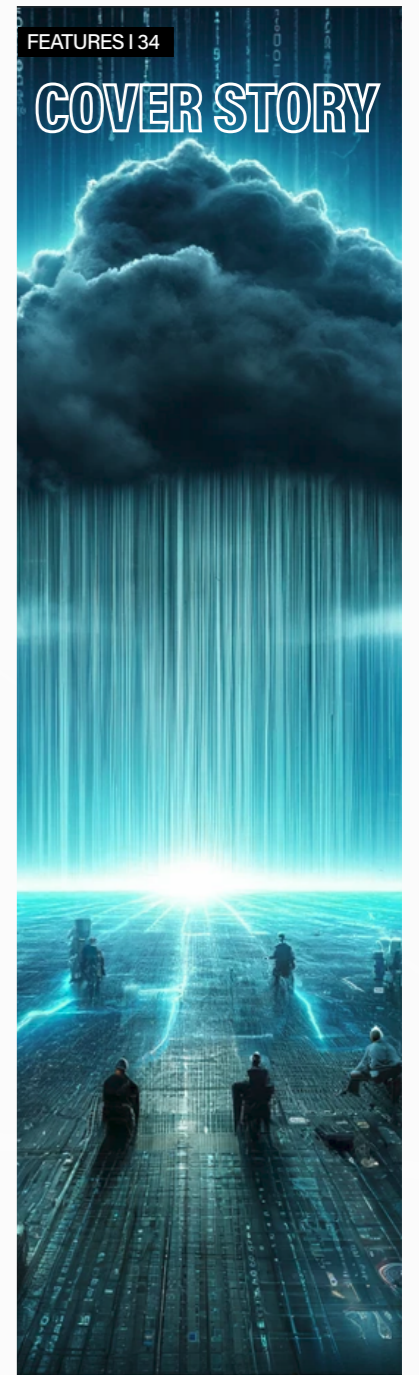
## EXPERT VIEWS Corner

### Page 40 - AI in Cybersecurity: Savior or Threat?

Explore the dual-edge AI in cybersecurity

### Page 41 - GDPR and Beyond: How compliance is shaping cybersecurity strategies?

Examine the impact of GDPR on cybersecurity strategies



Page 42 **PowerShell Automation and Scripting for Cybersecurity**



Page 43 **Practical Cybersecurity Architecture - Second Edition**



# TABLETOP EXERCISES: SIMULATING CYBER ATTACKS TO ENHANCE INCIDENT PREPAREDNESS

**Danny Abramovich**  
CEO of Titans Security Group

**I**n the digital age, cybersecurity threats loom larger than ever, making robust defense mechanisms critical for organizations across the globe. Among the most effective strategies to bolster cybersecurity defenses is the implementation of tabletop exercises. These simulations of cyber attack scenarios provide a unique and invaluable opportunity for organizations to test their incident response capabilities, ensuring preparedness in the face of real-world threats.

## What Are Tabletop Exercises?

Tabletop exercises are structured discussions conducted in a classroom

setting, designed to simulate a series of realistic cybersecurity scenarios. Unlike live drills or technical simulations, tabletop exercises focus on

the strategic, decision-making process, requiring participants to navigate hypothetical but plausible cyber incidents. These exercises bring together

key stakeholders from various departments, including IT, security, legal, and executive teams, to collaboratively respond to simulated threats, making critical decisions in a controlled environment.

## The Benefits of Conducting Tabletop Exercises

The advantages of conducting tabletop exercises are manifold. Firstly, they enhance communication and collaboration across different organizational levels, breaking down silos that can impede effective incident response. Participants gain a deeper understanding of their roles and responsibilities during a cyber incident, fostering a cohesive and coordinated response strategy. Additionally, these exercises highlight potential gaps in an organization's incident response plan, providing a clear roadmap for fortification. By simulating the stress and urgency of a real cyber attack, tabletop exercises also allow teams to practice maintaining composure and making informed decisions under pressure.

## Designing a Tabletop Exercise: Key Components

Creating an effective tabletop exercise begins with clear objectives. What specific threats or weaknesses does the organization aim to address? Once goals are established, crafting realistic scenarios is crucial. These should reflect potential threats relevant to the organization's industry and technological infrastructure. Key components include a detailed narrative, specific challenges for participants to

overcome, and predefined roles for each participant, ensuring a comprehensive evaluation of the organization's incident response capabilities.

## Examples Scenarios for Tabletop Exercises

A well-designed scenario is pivotal for a successful tabletop exercise. Here are detailed examples:

- **Ransomware Attacks:** The scenario begins with the IT department detecting unusual network activity. Soon after, critical systems are encrypted, and a ransom note appears. Participants must navigate crisis communication, legal considerations, and recovery efforts without paying the ransom.
- **Data Breach:** This scenario involves the unauthorized access and exfiltration of sensitive customer data. Teams are tasked with assessing the scope of the breach, mitigating damage, and managing public relations alongside compliance with data protection laws.
- **DDoS Attacks:** Here, the organization faces a distributed denial of service (DDoS) attack, crippling its online services. The exercise focuses on restoring services, identifying the attack's source, and communicating with stakeholders throughout the incident.

## Best Practices for Conducting Tabletop Exercises

For tabletop exercises to be truly effective, engagement

and realism are key. Facilitators should encourage active participation from all attendees, ensuring that the scenario is treated with the seriousness of a real incident. Additionally, integrating feedback from previous exercises can enhance the realism and relevance of future simulations. It's also vital to vary the scenarios and challenges to cover a wide range of potential threats.

## Learning from Tabletop Exercises: Post-Exercise Analysis

The value of a tabletop exercise is fully realized in the debriefing session. This is where teams gather to discuss the exercise's outcomes, analyze decisions made, and identify areas for improvement. Insights gained from these discussions should inform updates to the incident response plan, closing any gaps and strengthening the organization's cybersecurity posture.

## Conclusion

Tabletop exercises stand as a cornerstone of comprehensive cybersecurity preparedness, offering a dynamic platform to test, refine, and enhance an organization's response to cyber incidents. Through careful design, execution, and follow-up, these exercises not only prepare teams for the challenges of cybersecurity threats but also foster a culture of continuous improvement and resilience. As cyber threats evolve, so too must our strategies to combat them, with tabletop exercises playing a pivotal role in ensuring organizations remain one step ahead.

# CYBER CRISIS LEADERSHIP: THE ROLE OF CISOs IN INCIDENT RESPONSE

Erez Levi  
CISO at Lusha



In an era where digital technologies underpin critical business operations, the specter of cyber threats looms larger than ever. These threats not only pose significant financial risks but also threaten the integrity and reputation of organizations. At the heart of the defense against this digital onslaught stands the Chief Information Security Officer (CISO), whose role in incident response and crisis management is pivotal. This article explores the multifaceted responsibilities of CISOs in steering their organizations through cyber crises, emphasizing their leadership, strategic insight, and operational command.

## Understanding the Cyber Threat Landscape

The cyber threat landscape is a complex and ever-evolving domain. Organizations today face a plethora of digital threats ranging from data breaches and ransomware attacks to sophisticated state-sponsored cyber espionage. The impact of these threats can be devastating, resulting in significant financial losses, compromised customer data, and eroded trust in the brand. It is against this backdrop that CISOs operate, tasked with the colossal challenge of safeguarding their organizations in an unpredictable cyber environment. Their success hinges not just on their ability to respond to incidents as they occur but also on their foresight in anticipating and mitigating potential threats.

## Tactical Challenges in Incident Response

CISOs face a myriad of tactical challenges during incident response, from identifying the scope of the breach to coordinating recovery efforts. They must make rapid

decisions on how to contain the threat, mitigate damages, and communicate with affected parties. This requires a deep understanding of the organization's IT infrastructure, as well as the latest cybersecurity technologies and threat intelligence.

## The Evolving Role of CISO's

Traditionally seen as guardians of IT security, CISOs today are strategic leaders who play a crucial role in business continuity and risk management. Their responsibilities have broadened to include developing cybersecurity policies, ensuring compliance, and leading incident response teams. This evolution reflects the growing understanding that cybersecurity is not just a technical issue but a critical business function that impacts the entire organization.

## Strategic Role of CISO's in Cybersecurity

Gone are the days when the CISO's role was confined to the IT department, focusing solely on technical security measures.

In today's business landscape, CISOs are strategic leaders, integral to the overall business strategy and its alignment with cybersecurity goals. This transformation reflects a broader understanding that cybersecurity is not just an IT issue but a critical business function that impacts every aspect of the organization. CISOs, therefore, must possess a deep understanding of their organization's business objectives and the potential cyber risks that could undermine those goals. This strategic outlook enables them to guide their organizations in making informed decisions about cybersecurity investments and policies.

## Building and Leading Resilient Teams

A key aspect of the CISO's role is building and leading resilient incident response teams. This involves selecting skilled professionals, providing ongoing training, and fostering a collaborative work environment. CISOs must ensure their teams are prepared to act swiftly and effectively, which includes conducting regular drills and

simulations. Team resilience also depends on the CISO's ability to inspire confidence and maintain morale during high-pressure situations.

### Preparation and Prevention: The First Line of Defense

Strategic planning is crucial, involving not just the IT department but cross-functional teams to ensure a comprehensive approach to incident response. Proactive preparation and prevention form the cornerstone of effective cyber crisis management. CISOs lead this charge by implementing comprehensive threat intelligence programs that monitor and analyze the global threat landscape for potential risks to their organizations. But their responsibility extends beyond mere surveillance; they must also foster a culture of security awareness throughout the organization. This involves regular training sessions, phishing simulations, and other educational initiatives to ensure that all employees understand their role in safeguarding the organization's digital assets.

Integral to these preventive efforts is the development and continual refinement of an incident response plan. This plan, which should be tailored to the specific needs and risks facing the organization, outlines the steps to be taken in the event of a cybersecurity incident. It encompasses the identification of key team members, the roles and responsibilities of various departments, and the protocols for communication both internally and externally. By regularly testing and updating

this plan, CISOs ensure that their teams are prepared to act decisively and efficiently when faced with a cyber incident.

### Leading Through a Crisis: CISO's In Action

When a cybersecurity incident occurs, the CISO's leadership is paramount. This phase often involves making rapid decisions under pressure, coordinating with cross-functional teams, and executing the incident response plan with precision. Effective CISOs exhibit a calm demeanor, clear thinking, and decisive action—all essential in the heat of a crisis. By leveraging their comprehensive understanding of their organization's IT infrastructure, they can guide their teams in isolating the threat, minimizing damage, and beginning the recovery process. CISOs also play a key role in stakeholder management, ensuring that executives, board members, and external partners are informed and engaged throughout the crisis.

### Communication: The CISO's Tool for Managing Stakeholder Expectations

Effective communication is a critical tool in the CISO's arsenal, especially during a cyber crisis. Clear, concise, and timely communication with internal stakeholders, including the IT team, executive leadership, and the board, ensures a unified response to the incident. Moreover, transparent and responsible communication with external stakeholders, such as customers, regulators, and the media, can help manage the situation publicly and maintain trust.

CISOs must balance the need for openness with the imperative to protect sensitive information. Crafting a communication strategy that includes predefined templates for crisis communication can streamline this process, ensuring that messaging is consistent and reflects the organization's commitment to transparency and security.



### Technology and Tools: Enhancing the CISO's Capabilities

To effectively monitor, detect, and respond to cyber threats, CISOs rely on a suite of technological tools and solutions. These may include advanced threat detection systems, cybersecurity incident response platforms, and automation tools that can streamline response processes. Additionally, leveraging cloud-based backups and disaster recovery solutions can significantly reduce recovery time and mitigate the impact of a cyber incident.

Investing in these technologies, along with regular training on their use, enhances the capabilities of the incident response team, enabling them to respond more effectively to incidents and reducing the overall risk to the organization.

### Post-Incident Recovery and Analysis

After a cyber incident has been contained and normal operations are beginning to resume, the

CISO's focus shifts to recovery and analysis. This phase involves a thorough investigation of the incident to understand how the breach occurred, the scope of the impact, and the effectiveness of the response. Learning from these incidents is crucial for strengthening cybersecurity measures and refining incident response plans.

CISOs lead this reflective process, ensuring that lessons learned are integrated into future security strategies. This may involve updating security policies, enhancing technical controls, or revising business continuity plans to better prepare for future incidents.

### Building a Resilient Cybersecurity Culture

Finally, CISOs play a vital role in cultivating a resilient cybersecurity culture within their organizations. This involves embedding cybersecurity awareness into the DNA of the organization, ensuring that every employee understands their role in maintaining the organization's cyber defenses. Regular training, engagement initiatives, and a

clear emphasis on cybersecurity from the top down are essential components of this cultural shift.

A strong cybersecurity culture not only enhances the organization's preparedness for cyber incidents but also fosters an environment where security is considered a shared responsibility, significantly reducing the risk of future breaches.

### Navigating Future Challenges

As cyber threats continue to evolve, CISOs must stay ahead of the curve, anticipating new types of attacks and adapting their strategies accordingly. This includes investing in advanced cybersecurity technologies, enhancing threat intelligence capabilities, and advocating for a security-first culture across the organization. Additionally, CISOs must navigate the challenges of regulatory compliance, ensuring that incident response efforts are aligned with legal and ethical standards.

## CONCLUSION

The role of the Chief Information Security Officer in navigating cyber crises is both complex and critical. Through strategic planning, effective communication, operational excellence, and a commitment to fostering a culture of cybersecurity resilience, CISOs play an indispensable role in protecting their organizations from the ever-evolving threats of the digital age. As cyber threats continue to grow in sophistication and impact, the leadership, skills, and strategies of CISOs will remain at the forefront of cybersecurity efforts, safeguarding the digital frontier. The journey ahead is complex, but with strong cyber crisis leadership, organizations can emerge from challenges stronger and more secure.



# AN EXCLUSIVE INTERVIEW WITH

**Mr. Yigal Akerman**  
CISO at DataLoop

## What do you consider the most significant cybersecurity threat today?

The most significant threat we're facing is the sophistication of cyber attacks, particularly those powered by AI and machine learning. Attackers are using these technologies to automate attacks, making them more

risk management, and even in shaping customer trust and business innovation.

## What measures do you take to ensure your company's data privacy and compliance?

Ensuring data privacy and compliance involves a multi-layered approach. We start

particularly effective is adopting a zero-trust architecture. By never assuming trust and always verifying, we significantly reduce our attack surface. This approach, combined with continuous monitoring and real-time threat intelligence, allows us to quickly detect and respond to threats before they can cause harm.

## In the event of a data breach, what immediate steps do you take to mitigate the damage?

In the event of a breach, our immediate step is to contain the breach to prevent further data loss. We then assess the scope and impact of the breach, notifying affected stakeholders

datasets to identify anomalies that would be impossible for humans to find, predicting and preventing potential threats. However, they also present new challenges, as attackers can leverage AI to develop more sophisticated attack methods. It's a double-edged sword that will shape the future of cybersecurity.

in industry forums and cybersecurity consortiums also helps us share knowledge and best practices. Continuous learning and adapting our strategies in response to new information is key to staying ahead.

## Looking forward, what emerging technology do you believe will have the biggest impact on cybersecurity?

Quantum computing poses both a significant challenge and opportunity for cybersecurity. Its potential to break current encryption standards will necessitate a complete overhaul of data protection strategies. However, it also offers new possibilities for secure communication through quantum encryption methods. Preparing for the quantum era is crucial for the future of cybersecurity.

## What's your approach to cybersecurity training for employees?

Our approach to cybersecurity training is continuous and interactive. We provide regular training sessions, simulations, and phishing exercises to keep security top of mind for our employees. Tailoring content to different departments ensures relevance, and gamifying elements of the training helps increase engagement. It's about creating a culture of security awareness throughout the organization.

## How do you stay ahead of the constantly changing cybersecurity landscape?

Staying ahead requires constant vigilance and a proactive mindset. We invest in threat intelligence platforms to gain insights into emerging threats and trends. Participating

“Balancing security with innovation requires a culture shift towards embracing security as an enabler rather than a blocker”



complex and harder to detect. The rise of ransomware as a service (RaaS) also poses a significant threat, as it allows even inexperienced criminals to launch devastating attacks.

## How has the role of a CISO evolved in the past few years?

The role of a CISO has evolved significantly, moving from a technical focus to a more strategic one. Today, a CISO is expected to understand not just the technical aspects of cybersecurity but also the business implications of security decisions. We're now integral to strategic planning,

with a robust data governance framework, classifying data based on sensitivity and regulating access accordingly. We implement strong encryption standards for data at rest and in transit. Additionally, we conduct regular audits and compliance training for employees to ensure adherence to regulations like GDPR, CCPA, and others relevant to our industry.

## Can you describe a cybersecurity strategy that has been particularly effective for your organization?

One strategy that has been

## How do you balance the need for security with the need for innovation and agility in the digital space?

becoming more strategic. Balancing security with innovation requires a culture shift towards embracing security as an enabler rather than a blocker. We foster close collaboration between security and development teams through DevSecOps practices, integrating security early in the development process. This not only enhances security but also ensures that it doesn't hinder agility and innovation.

and regulatory bodies as required. Simultaneously, we work on identifying the breach's cause to close any security gaps and prevent future incidents. Communication is key throughout this process, both internally and externally, to maintain transparency and trust.

## How do you see artificial intelligence and machine learning impacting cybersecurity in the next few years?

AI and ML will significantly transform cybersecurity by enhancing threat detection and response capabilities. These technologies can analyze vast



**Alen Hershko**  
Security Architect at Global-e, and Ex-CISO

**IN** today's rapidly evolving cyber threat landscape, proactive defense mechanisms have become paramount for organizations across all sectors. Cybersecurity threat intelligence services play a pivotal role in this new defensive strategy, offering a way to anticipate, identify, and mitigate potential threats before they can impact business operations. However, selecting the right service is crucial. This guide aims to provide a comprehensive overview to assist buyers in making informed decisions when choosing cybersecurity threat intelligence services.

### Understanding Cybersecurity Threat Intelligence Services

Cybersecurity threat intelligence services gather, analyze, and interpret information about potential cyber threats and vulnerabilities. This intelligence is not just raw data; it's contextual information that helps organizations understand the nature of threats, the tactics, techniques, and procedures (TTPs) of threat actors, and the implications for their specific context. A robust service offers actionable insights, enabling businesses to tailor their security measures effectively.

For instance, a high-profile retail corporation might use threat intelligence services to monitor for signs of credential stuffing attacks, a common threat to online retailers. By leveraging intelligence feeds that alert them to breaches involving similar businesses or to new credential stuffing tools being sold on the dark web, the corporation can preemptively strengthen their authentication processes.

### Key Characteristics and Properties

- **Comprehensive Coverage:** A top-tier service should offer wide-ranging coverage of the cyber threat landscape, including insights into geopolitical trends, industry-specific threats, and emerging vulnerabilities. This coverage ensures that

organizations are not blindsided by niche or evolving threats.  
**Example:** A global financial institution requires intelligence that covers not just generic cyber threats but also those specific to the financial sector, such as SWIFT system attacks. A suitable threat intelligence service for them would include insights from financial industry-specific forums, malware trends targeting banking software, and regulations affecting cybersecurity in the financial sector.

- **Real-Time Updates:** The dynamic nature of cyber threats necessitates real-time, or near-real-time, intelligence updates. Delayed information can significantly reduce the effectiveness of the intelligence, potentially leaving organizations exposed to fast-moving attacks.  
**Example:** During the WannaCry ransomware outbreak, organizations with threat intelligence services offering real-time updates were able to receive immediate notifications about the attack vector (SMBv1 vulnerability) and the available patches, significantly reducing their susceptibility to the attack.
- **Customizability and Relevance:** The ability to customize intelligence feeds and alerts based on specific organizational assets, industry sectors, or threat types is crucial.

Services should offer tailored intelligence that is directly relevant to the organization's unique threat profile and operational context.  
**Example:** An energy sector company might be particularly susceptible to attacks on industrial control systems (ICS). A customized threat intelligence feed focusing on ICS vulnerabilities, patches, and threats, including those specific to the energy sector, would be crucial for their security posture.

### Must-Have Features

- **Automated Data Collection and Analysis:** Automation in data collection and analysis ensures a breadth and depth of intelligence gathering that manual processes cannot match. This feature supports the identification of complex patterns and correlations across diverse data sources, enhancing the quality of the threat intelligence provided.  
**Example:** A service automates the collection of threat intelligence from hundreds of sources, including technical blogs, dark web forums, and malware repositories. Using AI, it analyzes this data to identify emerging threats, such as a new ransomware variant, and provides a comprehensive report on its mechanics, indicators of compromise (IoC), and mitigation strategies.



Integration Capabilities:

The service should seamlessly integrate with existing security tools and workflows, enhancing the organization's overall security posture without requiring significant overhauls of current systems. This includes compatibility with SIEM systems, firewalls, and endpoint protection platforms.

**Example:** A company uses a popular Security Information and Event Management (SIEM) system. The chosen threat intelligence service offers a plug-in that integrates directly with this SIEM, allowing real-time threat data to enhance alert accuracy and reduce false positives.

Actionable Insights:

Beyond identifying threats, the service must provide actionable insights for mitigation. This includes specific recommendations for countering identified threats, contextual analysis to understand the implications of threats, and guidance on prioritizing security efforts.

**Example:** Upon detecting a new phishing campaign targeting their industry, a threat intelligence service not only alerts the company but also provides detailed information on the email subjects used, the sender's IP address, and suggested email gateway rules to block the attack.

Expert Support and Analysis:

Access to human expertise is critical. The best services offer not just automated intelligence but also the opportunity to consult with cybersecurity experts for deeper analysis and tailored advice on complex threats and incidents.

**Example:** When faced with a complex, targeted attack, a business can consult directly with cybersecurity analysts from their threat intelligence provider. These experts help interpret the threat data, advise on specific defenses, and can even assist in incident response planning.

Benefits of Implementing Threat Intelligence Services

Proactive Security Posture:

Implementing threat intelligence services shifts an organization from a reactive to a proactive security posture. This proactive approach allows businesses to anticipate threats and prepare defenses in advance, reducing the likelihood and impact of cyber attacks.

**Example:** By utilizing threat intelligence to monitor for and analyze trends in DDoS attack vectors, an online gaming company can adjust its defenses before major product launches, ensuring high availability when it matters most.

Improved Incident Response:

With actionable intelligence, organizations can streamline their incident response processes. Having detailed information on potential threats allows for faster identification and mitigation of attacks, minimizing downtime and operational disruption.

**Example:** A threat intelligence service identifies a malware infection in its early stages within an organization. The detailed intelligence allows the security team to quickly isolate affected systems and remove the malware, minimizing the impact.

Strategic Security Planning:

Long-term benefits include the ability to plan security strategies with a forward-looking perspective. Organizations can allocate resources more efficiently, focusing on areas of highest risk and potential impact, based on trends and predictions provided by threat intelligence.

**Example:** Annual threat reports and industry-specific threat forecasts provided by the intelligence service enable a financial institution to plan its cybersecurity investments more strategically, focusing on areas of highest predicted risk, such as securing mobile banking applications.

What to Check with Vendors Before Buying

- Data Sources and Collection Methods:** Ask about the diversity and reliability of the vendor's data sources. Understanding how data is collected, and the breadth of that collection, can provide insights into the comprehensiveness of the intelligence service. **Example:** Asking a potential vendor about their data sources might reveal they use a combination of open-source intelligence (OSINT), commercial feeds, and proprietary data from a network of sensors and honeypots, offering a comprehensive view of the threat landscape.
- Customization and Scalability:** Determine the extent to which the service can be customized to fit your organization's needs and how easily it can scale as your business grows or as threats evolve. **Example:** For a rapidly expanding e-commerce platform, it's vital that the threat intelligence service can scale with their growth. During discussions, the vendor demonstrates how their service can be tailored to different regions and how additional feeds can be easily integrated as the company enters new markets.
- Delivery and Reporting Mechanisms:** Inquire about how intelligence is delivered (e.g., dashboards, reports, alerts) and the frequency of these deliveries.

The format should align with your organization's capacity to consume and act on the intelligence.

**Example:** A multinational corporation needs to distribute threat intelligence to various teams globally. They should look for a service that offers flexible delivery options, such as an API for custom integrations, email summaries for executive leadership, and in-depth reports for the security team.

- Compliance and Privacy:** Ensure that the vendor's practices comply with relevant data protection and privacy regulations, especially if the intelligence service involves sharing sensitive organizational data.

**Example:** A healthcare organization must ensure that any external service complies with healthcare-specific regulations like HIPAA. They would need to verify that the threat intelligence service has a track record of handling data in a manner compliant with these standards.

- Customer Support and Community:** Evaluate the level of customer support provided, including access to expert analysts. Additionally, consider whether the vendor fosters a community of users for sharing best practices and insights.

**Example:** A vendor offering dedicated support channels and a user community where clients can share strategies and insights could be highly

beneficial. During selection, finding out if there are user forums, regular webinars, and direct access to analysts can be a deciding factor.

Conclusion

Choosing the right cybersecurity threat intelligence service is a strategic decision that can significantly enhance an organization's security posture. By focusing on the key characteristics, must-have features, and benefits outlined in this guide, and by asking the right questions of potential vendors, organizations can select a service that not only protects against current threats but also prepares them for future challenges.



# DEMYSTIFYING THE ISO 27001:2022 REQUIREMENTS: 10 BASIC STEPS TO DEVELOP A FRAMEWORK FOR SETTING INFORMATION SECURITY OBJECTIVES

**Sapir Cohen**

GRC Manager at TITANS SECURITY



**T**he last version of the ISO 27001:2022 standard requires the development of a framework for setting information security objectives for the organization. Defining a framework for setting information security objectives involves establishing a structured approach to identifying, assessing, and prioritizing the goals guiding an organization's information security program. This framework ensures that security efforts align with business objectives and compliance requirements and that resources are allocated efficiently to address the most critical risks. Here is an overview of such a framework:

## 1 Understand Business Context

Begin by comprehensively understanding the organization's mission, values, strategic goals, and operational environment. This context provides the foundation for aligning information security objectives with business objectives. You must delve into the organization's strategic plans, market position, competitive landscape, and operational processes. This understanding should guide the prioritization of information security efforts. For example, a financial institution might prioritize transactional data security due to its direct impact on customer trust and regulatory compliance.

**Example:** A healthcare provider analyzes how it manages sensitive patient data, identifying critical operations, the technology used, and external factors like regulatory changes. This understanding helps in tailoring the ISMS to the specific needs, risks, and processes of the organization.

## 2 Identify and Classify Information Assets

Catalog all information assets (data, systems, technologies, and processes) and classify them based on their sensitivity, criticality, and value to the organization. This step helps in prioritizing assets that require the most stringent protection. For instance, patient records in a healthcare provider's database would be classified as highly confidential and integral, necessitating stringent protections.

**Example:** A financial institution lists all its information assets, including customer databases, internal policy documents, and server infrastructure. Each asset is then classified based on its confidentiality, integrity, and availability requirements.

## 3 Risk Assessment

Conduct a thorough risk assessment to identify potential threats and vulnerabilities that could impact the identified information assets. Assess the likelihood and impact of these risks, considering internal and external threat landscapes. Use methodologies such as OCTAVE, FAIR, or ISO 27005 to assess risks systematically. Identify potential threats (e.g., cyber-attacks, data leaks) and vulnerabilities (e.g., outdated software, weak passwords) and evaluate their potential impact. A retail company, for example, might identify point-of-sale systems as high-risk due to their direct access to customer payment information.

**Example:** An e-commerce company conducts a thorough risk assessment where threats to information security, such as cyber-attacks, data breaches, or system failures, are identified, and the potential impacts are evaluated to prioritize risk management efforts.

## 4 Regulatory and Compliance Requirements

Map out all relevant legal and regulatory frameworks like GDPR, HIPAA, or PCI DSS that the organization must adhere to. Understand the legal, regulatory, and contractual obligations related to information security that the organization must comply with. These requirements will significantly influence the setting of security objectives. For a multinational corporation, this might involve navigating a complex web of international data protection laws and ensuring compliance across different jurisdictions.

**Example:** A multinational corporation reviews applicable global data protection regulations (such as GDPR, HIPAA) to ensure its ISMS meets all legal, statutory, regulatory, and contractual requirements.

## 5 Stakeholder Engagement

Engage with key organizational stakeholders to gather insights on their security needs, concerns, and expectations. This includes executive leadership, IT, legal, HR, operations, and other relevant departments. Conduct workshops, interviews, and surveys with stakeholders to understand their security needs and perceptions. In a manufacturing company, engaging with plant managers might reveal specific concerns about intellectual property theft or industrial espionage.

**Example:** An IT services firm engages with various stakeholders, including customers, shareholders, and employees, to understand their expectations for information security, ensuring their concerns are addressed in the ISMS.

## 6 Define Security Objectives

Based on the business context, asset classification, risk assessment, and compliance requirements, define specific, measurable, achievable, relevant, and time-bound (SMART) information security objectives. These objectives should mitigate identified risks, protect critical assets, and ensure compliance with applicable standards and regulations. Develop clear objectives such as "Reduce the risk of data breaches by 50% within two years" or "Achieve ISO 27001 certification by Q3 2024." These objectives should be directly tied to mitigating identified risks and protecting critical assets. An objective for a software development firm might focus on securing the development lifecycle to prevent code vulnerabilities.

**Example:** A software development company defines specific, measurable security objectives, such as achieving zero data breaches for the year or ensuring all employees complete cybersecurity training bi-annually.

## 7 Strategy and Resource Allocation

Develop a strategic plan to achieve the objectives, outlining the required security measures, technologies, policies, and procedures. Outline strategies like adopting a Zero Trust architecture, implementing multi-factor authentication, or conducting regular security awareness training. Determine the resources (budget, personnel, technology) needed to implement these measures effectively. Allocate resources based on the criticality of the objectives. A small business might prioritize investing in cloud-based security solutions to get a better ROI compared to expensive on-premises infrastructure.

**Example:** A retail chain allocates resources for security improvements, which include investing in new encryption technology for its online transactions and hiring additional cybersecurity personnel.

## 8 Implementation Plan

Create a detailed implementation plan with timelines, responsibilities, and milestones for achieving the security objectives. This plan should include short-term, medium-term, and long-term activities. Develop a phased plan, for example, starting with quick wins like improving password policies and then moving on to more complex tasks like network segmentation. Assign clear responsibilities, such as appointing a data protection officer to oversee GDPR compliance efforts.

**Example:** A government agency outlines an implementation plan for its ISMS, detailing timelines, roles, and responsibilities for introducing new security policies, conducting training sessions, and upgrading physical security measures.

## 9 Performance Measurement and KPIs

Establish Key Performance Indicators (KPIs) and metrics to monitor and measure the effectiveness of the implemented security measures in achieving the set objectives. Define specific metrics such as the number of detected phishing attempts, the time to detect and respond to incidents, or the percentage of employees completing mandatory security training. A tech startup might monitor the frequency of security patches applied to their product as a KPI for product security. Regular monitoring and reporting are essential for transparency and accountability.

**Example:** A technology startup establishes KPIs for ISMS performance, such as the time taken to detect and respond to security incidents and the percentage of employees passing regular security awareness tests. Another tech startup might monitor the frequency of security patches applied to their product as a KPI for product security. Regular monitoring and reporting are essential for transparency and accountability.

## 10 Continuous Improvement

Implement a process for regular review and updating of the information security objectives and the overall framework in response to changes in the business environment, emerging threats, technological advancements, and lessons learned from security incidents. Learn from industry incidents; for example, if a similar organization suffers a breach due to a third-party vendor, re-evaluate and strengthen your own third-party risk management practices.

**Example:** An automotive manufacturer regularly reviews and updates its ISMS based on audit results, evolving threats, and feedback from internal and external audits, aiming for ongoing enhancement of its security posture.

Each of these steps is crucial for implementing a robust ISMS in line with ISO 27001, ensuring that information security is continuously managed, monitored, and improved according to the organization's evolving needs and external conditions.

# PRIVACY BY DESIGN - BUILDING SECURITY INTO THE DIGITAL BLUEPRINT

**Daniel Mikhailov**

Team Leader at Titans Security Group



**IN** our digital age, privacy concerns are at the forefront of consumers' minds, leading to a critical re-evaluation of how privacy is integrated into products and services from the ground up. Privacy by Design (PbD), a concept pioneered by Dr. Ann Cavoukian, offers a framework for protecting privacy by embedding it into the design specifications of technologies, business practices, and networked infrastructures. This article explores the seven foundational principles of PbD with detailed examples of their implementation.

## The Principles of Privacy by Design

At its core, PbD is governed by seven foundational principles:

### **P1# Proactive not Reactive; Preventative not Remedial**

Principle: Anticipate and prevent privacy-invasive events before they happen.

Example: A health app developer integrates strong data encryption and anonymous data processing right from the initial design phase. This pre-emptive approach prevents personal health information from being exposed, even in the event of a data breach.

### **P2# Privacy as Default Setting**

Principle: Privacy is assured automatically for all users without requiring them to take any action.

Example: A social media platform automatically sets profiles to the highest privacy settings upon user registration. Users must actively choose to make their profiles more public, ensuring that privacy is the default state.

### **P3# Privacy Embedded into Design**

Principle: Privacy is an integral part of the system, without diminishing functionality.

Example: An e-commerce website designs its checkout process to request only the essential information needed for the transaction, such as shipping details, and avoids unnecessary data collection like browsing history, ensuring privacy without sacrificing user experience.

### **P4# Full Functionality - Positive-Sum, not Zero-Sum**

Principle: It is possible to have both privacy and security without sacrifices, rejecting the notion that trade-offs are inevitable.

Example: A cloud storage service offers end-to-end encryption for file storage and sharing, ensuring users' privacy while maintaining the functionality of easy access and collaboration tools, demonstrating that privacy and utility can coexist.

**P5# End-to-End Security – Full Lifecycle Protection**

Principle: Strong security measures are applied throughout the entire lifecycle of the data, from collection to deletion.

Example: A mobile messaging app implements secure data handling practices, including encrypted storage of messages on servers and secure deletion protocols, ensuring messages are protected until they are permanently deleted from all stored locations.

**P6# Visibility and Transparency – Keep it Open**

Principle: All stakeholders are assured that whatever the business practice or technology involved, it operates according to the stated objectives and is subject to independent verification.

Example: A financial service company undergoes regular privacy audits by third-party organizations and publishes these audit reports, providing transparency about its data handling practices and reassuring users about their privacy.

**P7# Respect for User Privacy – Keep it User-Centric**

Principle: User privacy is respected by offering strong privacy defaults, appropriate notice, and empowering user-friendly options.

Example: An online retailer provides clear, concise information about how customer data will be used and offers easy-to-understand choices for users to control their own data, such as opt-in features for personalized marketing communications.

**Implementing Privacy by Design**

The implementation of PbD principles extends beyond policy and into the realm of practical, technical solutions. For instance, adopting “data minimization” strategies can significantly reduce privacy risks. An IoT device manufacturer might apply this by designing devices that only collect necessary operational data, rather than extraneous information that could compromise user privacy.

Furthermore, engagement with stakeholders, including customers, employees, and

partners, is crucial for the effective implementation of PbD. This involves clear communication about how privacy is protected, what data is collected, and how it is used. For example, a tech company might hold a webinar or publish a white paper detailing their PbD approach, illustrating their commitment to privacy.

**Implementing PbD in Software Development**

Integrating PbD principles into software development requires a paradigm shift. For instance, when developing a new application, developers should encrypt user data by default, ensuring that personal

information is protected if a breach occurs. Another example is the adoption of minimal data processing principles, where only the data necessary for a specific purpose is collected, thereby reducing the risk of misuse.

A practical application of PbD is seen in the development of “privacy-aware” user interfaces. For instance, a social networking platform might design its settings to default to the most private option, requiring users to actively choose to share information more broadly. This approach empowers users and embeds privacy into the product’s DNA.

**Implementing PbD on the Organizational Level**

Implementing PbD requires a multifaceted approach, encompassing both organizational strategies and specific development practices. Below I’ll elaborate on general strategies for implementing PbD across an organization, providing useful examples:

- **Data Protection Impact Assessments (DPIA’s):** Before launching new projects or making significant changes to existing ones, organizations should conduct DPIAs. This involves assessing the data processing operations to identify and mitigate privacy risks. For example, a company planning to introduce a new customer relationship management (CRM) system would analyze how customer data is collected, stored, accessed, and shared, ensuring that privacy risks are addressed before the system is deployed.
- **Privacy Training and Awareness:** Educating employees about privacy importance and the organization’s privacy practices is vital. An example could be regular training sessions for developers, marketing teams, and customer service representatives, focusing on how their roles impact data privacy and the organization’s PbD policies.
- **Vendor and Third-Party Management:** Organizations must ensure that their vendors and third-party service providers adhere to PbD

principles. This could involve conducting privacy audits of potential vendors or including PbD requirements in contractual agreements. For instance, a company might require a cloud service provider to demonstrate how they encrypt data at rest and in transit.

**Case Study: GDPR and PbD**

The General Data Protection Regulation (GDPR) in the European Union explicitly requires PbD, showcasing its global relevance. A notable example of GDPR’s impact is the case of a technology firm that redesigned its data processing activities to ensure compliance. This included conducting privacy impact assessments to identify and mitigate privacy risks in new projects and demonstrating PbD in action. Such measures not only enhance consumer trust but also protect companies from potential fines and reputational damage.

**Benefits and Challenges of PbD**

Adopting PbD offers numerous benefits, including enhanced customer trust, compliance with global privacy regulations, and potentially preventing costly data breaches. However, challenges remain, such as the initial investment in training and technology to implement PbD principles, and the ongoing need to balance functionality with privacy.

Despite these challenges, the long-term benefits of building privacy into the digital blueprint

are undeniable. Companies that adopt PbD principles can differentiate themselves in a competitive market, turning privacy into a selling point rather than a compliance headache.

**The Future of Privacy by Design**

As digital technology continues to evolve, so too will the approaches to implementing PbD. Emerging technologies such as blockchain present new opportunities for enhancing privacy through decentralized data management, offering a glimpse into the future of privacy-conscious design. Meanwhile, regulatory bodies worldwide are increasingly recognizing the importance of PbD, incorporating its principles into legislation such as the European Union’s General Data Protection Regulation (GDPR).

**Conclusion**

Privacy by Design is more than a concept; it’s a necessary evolution in the way we create, use, and think about technology. As digital transformation accelerates, the importance of embedding privacy and security into the very fabric of digital products and services cannot be understated. By adopting PbD principles, companies not only safeguard their customers’ data but also position themselves as leaders in the digital age. Looking ahead, Privacy by Design will undoubtedly play a pivotal role in shaping the future of technology, making it imperative for all stakeholders to embrace its principles today.

# BREAKING INTO CYBERSECURITY: SKILLS YOU NEED FOR THE DIGITAL AGE

**Bella Silony**  
GRC Analyst at SimplyCert

**I**n a world where digital threats are increasingly prevalent, the demand for skilled cybersecurity professionals has never been higher. Breaking into the field of cybersecurity, however, requires more than just a keen interest in technology; it demands a specific set of skills tailored to the digital age. This article outlines the critical skills aspiring cybersecurity experts need to develop to protect digital assets and information in an ever-evolving threat landscape.

## Technical Proficiency

**Understanding of Networks and Systems:**  
A solid understanding of how networks and systems operate

is the bedrock of cybersecurity. Knowledge of network protocols, architecture, and the various types of networks (LAN, WAN, WLAN, etc.) is essential. Familiarity with operating

systems, from traditional ones like Windows and Linux to mobile platforms, is also crucial, as these are often the targets of cyber attacks.

**Programming and Scripting:**  
While not all cybersecurity roles require advanced programming skills, familiarity with programming and scripting languages is incredibly beneficial. Languages such as Python, JavaScript, and PowerShell are widely used in automating security tasks, developing security tools, and identifying vulnerabilities.

**Cyber Threat Knowledge:**  
A deep understanding of the cyber threat landscape, including the types of malware, the tactics, techniques, and procedures (TTPs) of threat actors, and the lifecycle of cyber attacks, is vital. This knowledge enables cybersecurity professionals to anticipate, identify, and mitigate threats effectively.

## Analytical Skills

**Problem-Solving Ability:**  
Cybersecurity is fundamentally about solving complex problems. Professionals in the field must be able to think critically and creatively to find solutions to security challenges, often under significant pressure.

**Attention to Details:**  
Given the sophisticated nature of modern cyber threats, a meticulous attention to detail

is necessary. Cybersecurity professionals must be able to scrutinize code, logs, and system configurations to identify anomalies that could indicate a security breach.

## Incident Response and Forensics:

The ability to respond to cyber incidents swiftly and conduct forensic analysis is key. This involves understanding the indicators of compromise (IOCs), using forensic tools to analyze breaches, and applying strategies to contain and remediate attacks.

## Soft Skills

**Communication:**  
Effective communication is critical in cybersecurity. Professionals must be able to convey complex security concepts in a manner that is understandable to non-technical stakeholders. They also need to write clear, concise reports and documentation.

**Teamwork and Collaboration:**  
Cybersecurity is a team sport. The ability to work collaboratively with IT professionals, management, and external stakeholders is essential for devising and implementing effective security strategies.

**Ethical Integrity:**  
Given the sensitive nature of the work, ethical integrity is non-negotiable. Cybersecurity professionals must adhere to high ethical standards, ensuring the privacy and protection of data and systems they are entrusted with.

**Continuous Learning and Adaptability:**  
The cybersecurity landscape is constantly evolving, with new threats and technologies emerging regularly. A commitment to continuous learning and professional development is crucial. This includes pursuing certifications, attending workshops and conferences, and staying abreast of the latest trends and best practices in the field.

**Specialized Skills:**  
As you progress in your cybersecurity career, consider developing specialized skills in areas such as penetration testing, cybersecurity analysis, security architecture, or cyber law and policy. Specialization can make you more attractive to employers and open up opportunities for advancement in the field.

## CONCLUSION

Breaking into cybersecurity requires a blend of technical proficiency, analytical skills, soft skills, and a commitment to continuous learning. By developing a strong foundation in networks and systems, honing your programming and problem-solving abilities, and cultivating effective communication and teamwork capabilities, you can position yourself as a valuable asset in the fight against cyber threats. Remember, the path to becoming a cybersecurity professional is a journey of lifelong learning, where curiosity, resilience, and ethical integrity will be your best allies. Welcome to the exciting world of cybersecurity, where you have the power to make a difference in the digital age.

# THE RESILIENT ENTERPRISE: ALIGNING CYBERSECURITY WITH BUSINESS CONTINUITY GOALS

**Shmaya Texon**

Business Continuity Manager at Discount Bank

**I**n today's digital landscape, where cyber threats loom large and operational complexities grow, the fusion of cybersecurity and business continuity has never been more crucial. The resilience of an enterprise hinges on its ability to prevent, respond to, and recover from cyber incidents while maintaining uninterrupted business operations. This article explores the synergy between cybersecurity and business continuity goals, laying the groundwork for building a resilient enterprise.

## Understanding the Interconnection

The digital age has ushered in a wave of technological advancements, along with an ever-expanding threat landscape. Cybersecurity incidents can range from data breaches to sophisticated ransomware attacks, each capable of causing significant operational disruption. It's this potential for disruption that tightly intertwines cybersecurity with business continuity. Cyber resilience emerges as a strategic imperative, integrating the proactive defense mechanisms of cybersecurity with the adaptive recovery strategies of business continuity planning.

## Strategic Alignment: Cybersecurity and Business Continuity

Achieving resilience requires a harmonious alignment between cybersecurity initiatives and business continuity strategies. This alignment ensures that an organization can not only withstand cyber threats but also sustain essential functions under adverse conditions. Key to this process is a comprehensive risk assessment, identifying potential cyber threats alongside other business risks, thereby facilitating a unified approach to organizational defense and recovery strategies. This integrated perspective is essential for developing a cohesive plan that addresses both cyber threats and business continuity needs.

## Implementing a Resilient Cybersecurity Framework

At the heart of a resilient enterprise lies a robust cybersecurity framework, designed to safeguard critical assets while ensuring operational continuity. This framework encompasses a range of components, including advanced threat detection, data encryption, secure backup solutions, and incident response protocols. Leveraging cutting-edge technologies like AI and machine learning for threat intelligence and anomaly detection can significantly enhance an organization's defensive posture. Successful case studies highlight how organizations have bolstered their resilience by adopting comprehensive cybersecurity measures, seamlessly integrated with their business continuity plans.

## Cultivating a Culture of Resilience

Beyond technological and procedural measures, the foundation of a resilient enterprise is its culture. Leadership plays a pivotal role in cultivating this culture, emphasizing the importance of cybersecurity awareness and resilience across all organizational levels. Effective training and awareness programs empower employees to recognize and respond to cyber threats, reinforcing the human element of cybersecurity defenses. This culture of resilience not only enhances the organization's capacity to deal with cyber incidents but also ingrains

the principles of business continuity into the corporate ethos.

## Monitoring, Testing, and Continuous Improvement

Resilience is not a one-time achievement but a continuous journey. Regular monitoring and testing of both cybersecurity defenses and business continuity plans are vital to ensuring their effectiveness over time. Simulated cyberattacks and business disruption scenarios can help identify vulnerabilities, providing insights for strengthening resilience. Moreover, staying abreast of emerging threats and evolving technologies enables organizations to adapt and improve their resilience strategies proactively.

## Conclusion

Aligning cybersecurity with business continuity goals is essential for building a resilient enterprise. This strategic integration not only enhances the organization's defensive capabilities against cyber threats but also ensures the sustainability of critical business functions during and after a cyber incident. By taking proactive steps towards this alignment, organizations can fortify their defenses, cultivate a culture of resilience, and navigate the complexities of the digital world with confidence. Embracing resilience is not just a strategic choice; it's a necessity for survival and success in today's interconnected and unpredictable business landscape.

# THE DIGITAL FRONTIER: NAVIGATING THE CYBERSECURITY LANDSCAPE IN 2024

**Or Levi**  
Co-Founder of Simplycert

**AS** we venture deeper into the 21st century, the digital frontier expands with unprecedented speed, becoming an integral part of our daily lives. In 2024, our reliance on digital technologies has surged, opening new avenues for innovation and connection. However, this digital expansion also paves the way for sophisticated cyber threats, making cybersecurity more crucial than ever. The landscape of cybersecurity is constantly evolving, challenging individuals and organizations to stay one step ahead of threats. This article delves into the cybersecurity landscape of 2024, highlighting emerging threats, the role of artificial intelligence (AI) and automation, global cybersecurity efforts, and practical tips for safeguarding digital assets.

## Emerging Cyber Threats in 2024

The year 2024 has witnessed the emergence of new cyber threats, fueled by advancements in technology. Cybercriminals now leverage AI and machine learning to orchestrate attacks with unprecedented precision and stealth. Phishing attacks have become more sophisticated, using deepfake technology to impersonate trusted figures. Ransomware attacks continue to evolve, targeting not just businesses but critical infrastructure, posing a significant threat to national security. These developments necessitate a proactive and dynamic approach to cybersecurity, highlighting the need for advanced detection and defense mechanisms. Here are some examples of these emerging threats:

- AI-Powered Phishing Attacks:** Phishing attacks have been around for years, but in 2024, they've become significantly more sophisticated thanks to artificial intelligence (AI). Cybercriminals are using AI algorithms to create highly convincing fake emails and messages that mimic the style and tone of communication of trusted individuals or organizations. These AI-powered phishing attempts can analyze a user's correspondence patterns and craft personalized messages that are incredibly difficult to distinguish from legitimate communications. This makes them much more effective and dangerous, potentially leading to unauthorized access to sensitive information.
- Deepfake Technology in Social Engineering:** Deepfake technology, which uses AI to create realistic video and audio recordings of real people saying or doing things they never did, has been adopted by cybercriminals for social engineering attacks. In 2024, attackers use deepfakes to impersonate company executives, public figures, or family members in video calls or audio messages to coerce victims into transferring funds, divulging confidential information, or granting access to secure systems. The realism of deepfake technology poses a significant challenge for individuals and organizations to distinguish between genuine and fabricated interactions.
- Quantum Computing and Encryption:** With the advent of quantum computing, traditional encryption methods are under threat. Quantum computers have the potential to break current encryption algorithms much faster than classical computers. In 2024, the fear is not only that nation-states could be developing quantum capabilities to undermine national security systems but also that cybercriminals might gain access to quantum computing services offered through the cloud, enabling them to decrypt sensitive data. This emerging threat has prompted the development of quantum-resistant encryption methods, although transitioning to these new standards is a complex and ongoing challenge.
- Smart Device Exploits in the IoT Ecosystem:** The Internet of Things (IoT) continues to expand in 2024, with billions of connected devices in homes, offices, and public spaces. While these devices offer convenience and efficiency, they also present new vulnerabilities. Cybercriminals are exploiting weak security in IoT devices for various malicious purposes, including forming botnets to launch distributed denial-of-service (DDoS) attacks, spying on users through insecure cameras or microphones, and gaining unauthorized access to broader networks. The diversity and quantity of IoT devices make it challenging to secure the ecosystem effectively.
- Supply Chain Cyber Attacks:** Supply chain attacks have become a major threat in 2024, where attackers target less-secure elements in the supply chain to compromise the final product or service. This can include infiltrating a software provider to add malicious code to an update or compromising hardware components at the manufacturing stage. These attacks can be highly effective because they exploit the trust between suppliers and customers. The interconnectedness of services and the reliance on third-party vendors in modern business amplify the potential impact of these attacks, affecting multiple organizations simultaneously.
- AI Model Poisoning:** AI and machine learning models are increasingly used for security applications, from malware detection to anomaly analysis. However, these models themselves have become targets. Attackers



are finding ways to feed these systems poisoned data to skew their learning processes, leading to incorrect outputs or decisions. This can degrade the performance of security systems or even turn them against their users, such as by classifying malicious activity as benign. The subtlety of these attacks makes them particularly insidious and hard to detect.

These emerging cyber threats in 2024 illustrate the ongoing arms race between cyber defenders and attackers. The complexity and sophistication of these threats require equally sophisticated responses, including advanced AI-driven defenses, robust encryption standards, and a proactive approach to security across the digital landscape.

### The Role of AI and Automation in Cybersecurity

AI and automation stand at the forefront of the battle against cyber threats in 2024. These technologies offer the ability to analyze vast amounts of data for suspicious activities, predict potential threats, and automate responses to security incidents. AI-driven security systems can adapt to new threats more quickly than traditional systems, providing a dynamic defense mechanism. However, this reliance on technology also presents challenges, such as the potential for AI systems to be manipulated by cybercriminals. Despite these challenges, the benefits of AI and automation in enhancing cybersecurity are undeniable, offering a critical tool in the

defense against cyber threats. The integration of Artificial Intelligence (AI) and automation into cybersecurity strategies has become a cornerstone in the defense against cyber threats. As the cyber threat landscape evolves with increasingly sophisticated attacks, AI and automation offer dynamic, intelligent solutions that can adapt and respond in real-time. Here are detailed examples illustrating the role of AI and automation in enhancing cybersecurity:

- Anomaly Detection and Behavioural Analysis:** AI-driven systems are exceptionally adept at monitoring network traffic and identifying unusual patterns that could indicate a security breach. By analyzing vast amounts of data, these systems can learn what normal network behaviour looks like and flag anomalies that deviate from the norm. For example, if a network that typically experiences low traffic volumes suddenly has a surge in activity, an AI system can alert security teams to a potential DDoS (Distributed Denial of Service) attack. Similarly, AI can detect subtle signs of insider threats, such as unusual file access or data transfers, by analyzing user behavior over time and identifying actions that stray from established patterns.
- Predictive Threat Intelligence:** AI algorithms can process and analyze data from multiple sources, including past security incidents, to predict future threats and vulnerabilities. This predictive

capability allows organizations to proactively address potential security gaps before they can be exploited. For instance, an AI system might analyze trends in phishing email tactics and predict a new variation that is likely to emerge, enabling cybersecurity teams to update their defenses and training materials accordingly.

- Automated Incident Response:** Automation in cybersecurity streamlines the response to detected threats, reducing the time from detection to mitigation. Automated security orchestration platforms can execute a series of predefined actions when a threat is detected, such as isolating infected devices, blocking malicious IP addresses, and deploying patches to vulnerable systems. This rapid response capability is critical in minimizing damage from attacks, especially outside of regular working hours when human response times might be slower. For example, if ransomware is detected on a network, an automated system can immediately quarantine the affected device and initiate a backup restoration process, significantly limiting the ransomware's impact.
- Enhanced Phishing Detection:** AI algorithms are increasingly effective at detecting phishing attempts that might evade traditional spam filters. By analyzing the language, sender information, and embedded links in emails, AI systems can identify subtle signs of phishing, such

as slight misspellings in domain names or unusual sender behaviour. This level of analysis goes beyond simple keyword matching, incorporating a nuanced understanding of phishing tactics to catch sophisticated attempts that might fool an unwary recipient.

- Security Policy Enforcement:** Automation tools play a crucial role in enforcing security policies across an organization's digital assets. They can automatically apply security configurations, enforce password policies, and ensure that only authorized devices can access the network. This helps maintain a consistent security posture even as the organization scales and reduces the risk of human error leading to security vulnerabilities. For instance, if an employee tries to connect a non-compliant device to the corporate network, an automated system can block access until the device meets the organization's security standards.
- Vulnerability Management:** AI and automation greatly enhance vulnerability management by continuously scanning for vulnerabilities in software and hardware, prioritizing them based on potential impact, and automating patch deployment processes. This proactive approach ensures that vulnerabilities are addressed promptly, reducing the window of

opportunity for attackers. For example, an AI system could identify a newly disclosed vulnerability in a widely used software package, assess which systems within an organization are affected, prioritize the vulnerability based on potential impact, and initiate the patching process—all without human intervention.

These examples underscore the transformative impact of AI and automation on cybersecurity. By enhancing detection capabilities, streamlining responses, and ensuring consistent policy enforcement, AI and automation not only improve an organization's security posture but also allow cybersecurity teams to focus on strategic initiatives and complex threat analysis, leveraging their expertise where it is most needed.

### Global Cybersecurity Efforts and Collaborations

In response to the global nature of cyber threats, 2024 has seen increased efforts and collaborations among nations to strengthen cybersecurity defenses. International agreements on cyber norms and cooperation in cybercrime investigations have enhanced the collective security posture. Countries are sharing intelligence on cyber threats and best practices for defense, fostering a collaborative environment to tackle the challenges of cybersecurity. These global efforts underscore the recognition that cybersecurity is

not just a national concern but a global imperative.

### Practical Tips for Navigating the Cybersecurity Landscape

Navigating the cybersecurity landscape in 2024 requires vigilance and proactive measures. Individuals and organizations should adopt a multi-layered security approach, combining technology, policies, and education to protect against threats. Regularly updating software, using strong, unique passwords, and being cautious of suspicious emails and links are fundamental practices. Additionally, staying informed about the latest cyber threats and security trends is essential for anticipating and mitigating risks. Organizations can benefit from conducting regular security audits and employee training to foster a culture of cybersecurity awareness.

In conclusion, the cybersecurity landscape of 2024 is characterized by the rapid evolution of digital technologies and the corresponding rise in sophisticated cyber threats. The integration of AI and automation into cybersecurity strategies offers promising solutions, but also presents new challenges. Global collaboration and adherence to best practices are key to navigating this complex landscape. By staying informed and adopting a proactive approach to cybersecurity, individuals and organizations can protect themselves against the threats of the digital frontier.

# FORECASTING THE STORM: THE FUTURE OF CYBER THREAT INTELLIGENCE

**Shahar Avenstein**  
CISO at SAM Seamless Networks

**I**n an era where digital landscapes are continually evolving, the necessity for robust cybersecurity measures has never been more paramount. As cyber threats become more sophisticated, the role of cyber threat intelligence (CTI) in preempting and mitigating these threats is increasingly critical. This article delves into the future of cyber threat intelligence, exploring how emerging technologies, evolving threat landscapes, and the integration of artificial intelligence (AI) are shaping its trajectory.

## The Evolving Threat Landscape

The cyber threat landscape is a chameleon, constantly changing hues to adapt and

overcome existing security measures. Ransomware, once a blunt tool for digital extortion, has evolved into highly targeted attacks against critical infrastructure and multinational

corporations. Simultaneously, the proliferation of Internet of Things (IoT) devices has expanded the attack surface, offering new avenues for cybercriminals to exploit.

State-sponsored cyber warfare has also escalated, with nations leveraging cyber espionage and sabotage as extensions of their geopolitical strategies. These evolving threats demand a more dynamic and predictive approach to cybersecurity, where threat intelligence plays a pivotal role.

## The Role of AI in Cyber Threat Intelligence

AI is at the forefront of transforming CTI, offering unparalleled speed and efficiency in processing vast datasets. Machine learning algorithms can identify patterns and anomalies within this data, predicting potential threats before they materialize. For instance, AI can analyze historical cyber attack data to forecast future threats, enabling organizations to fortify their defenses proactively.

Moreover, AI-driven natural language processing (NLP) tools are enhancing the capability to sift through unstructured data sources, such as blogs, forums, and social media, to gather intelligence about emerging threats and hacker tactics. This real-time, AI-enhanced intelligence is crucial for staying one step ahead of cyber adversaries.

## Emerging Technologies Shaping CTI

Quantum computing presents both a challenge and an opportunity for cyber threat intelligence. On one hand, it threatens to break the current cryptographic safeguards protecting sensitive data. On the other, it offers new methods for secure communication and data protection, potentially revolutionizing CTI by enabling the encryption of data in ways

that are currently unimaginable.

Blockchain technology is another area impacting CTI. With its inherent security features, such as decentralization and encryption, blockchain offers a promising platform for sharing threat intelligence securely and efficiently among different entities without the risk of tampering or interception.

## Integration and Collaboration

The future of CTI lies not only in technology but also in collaboration. Information sharing between public and private sectors can provide a more comprehensive view of the cyber threat landscape. Initiatives like the Cyber Threat Alliance (CTA) exemplify how collaboration can enhance the effectiveness of CTI by pooling resources and intelligence.

Moreover, integrating CTI with other cybersecurity practices, such as incident response and risk management, creates a holistic security posture that can adapt to and mitigate evolving threats. This integration ensures that intelligence is not just collected but is actionable, guiding strategic decisions and operational responses.

## The Human Element

Despite advancements in AI and technology, the human element remains irreplaceable in CTI. Skilled analysts interpret data, provide context, and make judgment calls where algorithms cannot. The future will likely see a hybrid model where AI handles the heavy lifting of data processing and analysts focus on strategic analysis and decision-making.

Furthermore, education and training in CTI will become increasingly important as the demand for skilled professionals grows. Organizations will need to invest in developing the next generation of cyber intelligence analysts who can navigate the complex interplay between technology, cybersecurity, and global geopolitics.

## Challenges Ahead

While the future of CTI is promising, it is not without challenges. Privacy concerns, especially regarding the collection and use of data for intelligence purposes, will need to be addressed. Balancing the need for comprehensive threat intelligence with respect for individual privacy rights will be a continuing challenge.

Additionally, the democratization of AI and machine learning tools means that cybercriminals can also leverage these technologies for malicious purposes. Counteracting AI-enhanced threats will require ongoing innovation and adaptation within the field of CTI.

## Conclusion

As we forecast the storm on the horizon, it's clear that the future of cyber threat intelligence is a bright but challenging one. Embracing AI and emerging technologies, fostering collaboration, and emphasizing the human element are all crucial for the development of CTI. By staying adaptive, proactive, and resilient, the field of cyber threat intelligence will continue to be a cornerstone of cybersecurity strategy, safeguarding digital realms against the ever-evolving threat landscape.

# RISK ASSESSMENT IN INDUSTRIAL CONTROL SYSTEMS AND OT NETWORKS THAT CONTROL HAZARDOUS MATERIALS

**Yosi Shavit**

CISO Head of ICS Cyber Security Dept. at the Israeli Ministry of Environmental Protection

## Calculating the cyber risk level in the Hazmat Industry

Risk management is based upon the risk assessment that reflects the vulnerability level of computer systems, the assessment of the threats, their potential consequences, and the probability of their occurrence.

The possible scenarios will be inspected according to the principle of "looking through the eyes of the assailant" because behind every cyber-attack there is a human attacker. The way to best resolve cyber security requires a deep understanding of the ways an attacker might operate, how to identify them, and how to prevent them.

The assumption is that during a malicious cyber-attack, most of the hazardous substance will be released in the component that contains the largest amount in the hazardous process that is connected to the computer system (as opposed to a release following a malfunction or an accident), and therefore calculations as to the dispersion of the hazardous substances will be made accordingly.

## Calculating the Risks

The risks are based on the relevant threats to the components of each system according to the risk analysis carried out by the business.

In calculating the risk, we have to calculate the 2 following parameters:

- 1. Impact level (I)** A risk assessment begins with an assessment of the impact

level that might be caused to the environment or public health if a hazardous substance event occurs following a cyber-attack. The impact level will be assessed at a range between 1 and 4 according to the method presented in the table provided in this article. Please note that the score determined at this stage is for the maximum impact level.

- 2. Exposure level (P).** After calculating the expected impact level of a hazardous substance event caused by a cyber-attack on the business, the exposure level must be calculated, the probability of a cyber event in systems that manage/control hazardous substances. That calculation is performed in this article.

## Calculating the risk assessment and the classification of the systems in the business

The risk level assessment is based upon a weighted calculation of the impact level expected given the probability that the impact will occur, according to the following formula:

$$\text{Risk} = P + 3 * I$$

## The risk is equal to the exposure level added by three times the impact level 2

We multiply I by 3 to give the value of I more influence because we are talking about public health and human life.

The greater the impact, the greater the risk, and the greater the risk, the greater the number of controls that need to be implemented.

**(I)** = The expected impact level concerning the worst-case scenario

**(P)** = The probability that the impact will occur

Application of the formula specified herein above for calculating the risk level will create a score of between 4 and 16.

Each one of the computer systems in the business that manages / controls hazardous substances will be classified into one of four groups according to its risk assessment, as specified herein below:

- Level 1 (Green):** A low risk potential (a score between 4 and 7).
- Level 2 (Yellow):** A medium risk potential (a score between 8 and 11).
- Level 3 (Orange):** A high risk potential (a score between 12 and 14).
- Level 4 (Red):** A very high-risk potential (a score between 15 and 16).

## The Heat Map

The following heat map describes the risk level as a function of the impact and exposure level:

Impact level (I)	4	3	2	1
Exposure level (P)				
4	16	13	10	7
3	15	12	9	6
2	14	11	8	5
1	13	10	7	4

### Number of Controls to implement

The number of controls to be assimilated at every risk level. Note that each control level includes the controls of the previous levels, for example control level 4 includes all the possible controls of levels 1, 2, 3, 4.

The risk potential	The controls package according to the risk potential	The number of controls for that level
4 -7	1	A <sup>3</sup>
8 -11	2	B
12 -14	3	C
15 -16	4	D

### Determining the controls that are required to be implemented

After calculating the risk level of the process, the business will know what control package it must implement according to the key provided herein below:

- Risk level at values of 4 through 7: Controls package 1.
- Risk level at values of 9 through 11: The controls package from level 2 (that includes the controls from levels 1 and 2).
- Risk level at values of 12 through 14: The controls package from level 3 (that includes the controls from level 1, the controls from level 2, and the controls from level 3).
- Risk level at values of 15 through 16: The controls package from level 4 (that includes the controls from level 1, the controls from level 2, the controls from level 3, and the controls from level 4).

The framework of the controls that are based on the cyber security framework (the NIST CSF framework) is comprised of five functions as follows:

- **Identify** - risk identification that includes mapping of the hazardous substances connected to the computer systems that manage/control hazardous substances and performance of a risk assessment of such systems.
- **Protect** - assimilation of controls according to the risk level obtained in the risk assessment to minimize as much as possible the probability of a cyber event that would cause a hazardous substance event.
- **Detect** - assimilation of capabilities to identify an existing attack or
- **Respond** - a response to an event, after the event has occurred.
- **Recover** - recovery from the event and resuming routine operation.

Understanding the importance of protecting both the OT and IT realms is crucial for comprehensive cybersecurity measures.

The required controls are primarily intended to protect the OT network and industrial control systems. However, it's important to understand that we also need to address the attack vector from the IT realm. Therefore, some of the controls should deal with this issue (such as remote connections to the OT network from the IT network, the use of ERP

systems sitting in the IT realm and transmitting work orders to the OT network, etc.).

### How to calculate the impact (I)?

The level of impact will be the highest value given in the "score" column.

The maximum impact is calculated by the CIA TRIAD, which is the basis for information security, and includes the safety (S) component, as a cyber-attack on computerized control systems dealing with hazardous materials. It's important to note that in the scenario of an attack on industrial control systems containing hazardous materials, we consider the worst-case scenario (WCS).

In scenarios involving hazardous material incidents, we consider the following scenarios:

- **Dispersion of hazardous materials** into the air, measured in parts per million (PPM).
- **Heat radiation** resulting from the ignition of hazardous materials, calculated in kilowatts per square hour.
- **Pressure effects** caused by the explosion of hazardous materials, calculated in units of pressure (BAR).

We can accurately calculate these values using software programs designed for this purpose. For example, there's software like Aloha that specializes in these calculations.

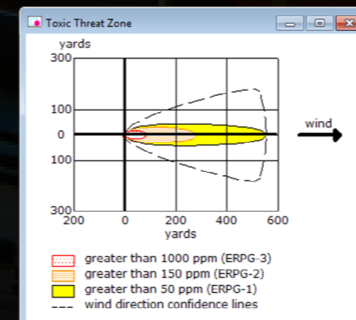
We can download the Aloha

software for free from the website of the United States Environmental Protection Agency (EPA) at: <https://www.epa.gov/cameo/aloha-software>

As of the writing of this article, the latest version is indeed 5.4.7.

ALOHA® (Areal Locations of Hazardous Atmospheres) is the hazard modeling program for the CAMEO® software suite (Computer-Aided Management of Emergency Operations), which is used widely to plan for and respond to chemical emergencies.

ALOHA allows you to enter details about a real or potential chemical release, and then it will generate threat zone estimates for various types of hazards. ALOHA can model toxic gas clouds, flammable gas clouds, BLEVEs (Boiling Liquid Expanding Vapor Explosions), jet fires, pool fires, and vapor cloud explosions. The threat zone estimates are shown on a grid in ALOHA, and they can also be plotted on maps in MARPLOT® (Mapping Application for Response, Planning, and Local Operational Tasks), Esri's ArcMap, Google Earth, and Google Maps. The red threat zone represents the worst hazard level, and the orange and yellow threat zones represent areas of decreasing hazard.<sup>4</sup>



The diagram above shows the impact zones in public scenarios: the red circle represents the range where human fatalities may occur, the orange circle indicates an area where there is irreversible health damage, and the yellow zone is an area where there is reversible damage (which can be treated, and the person can recover).

### How to calculate the max impact level (I)?

To calculate the value of the max impact (I), we need to answer 4 basic questions related to safety, confidentiality, integrity, and availability. The value is categorized between 1 to 4 (1 is the lowest, and 4 is the highest). The highest value (SCORE) obtained is the value of the Impact Level (I).

### How to calculate the exposure level (P)?

To calculate the exposure level (P), a response must be provided to 36 predefined questions by providing a score between 1 to 4 (1 is the lowest, and 4 is the highest). After assigning a score to all the questions, the exposure level will be calculated by summing up all the scores and calculating the average of the entire answers. The result obtained is the exposure level (P).

The analysis will be carried out according to this method relating to each process noted in the hazardous processes analysis and related to each computer system in each of those processes.

A formalized table is available per request, containing all questions and parameters for calculating both the impact and the exposure factors.

The table was constructed by the article's author through piloting risk assessments in various sectors, along with personnel from different areas of the production floor: control and ICS systems personnel, and OT personnel. Personnel from the chemistry and hazardous materials department also contributed to the construction of this table.

If you are interested in the detailed article, including the table with all questions for measuring the potential impact and exposure, you can use the following link: <https://www.consulting.titans-security.com/post/risk-assessment-in-industrial-control-systems-and-ot-networks-that-control-hazardous-materials>



## AI in Cybersecurity: Savior or Threat?

**Monas Shmuel**  
CISO at Local Government

In the rapidly evolving world of technology, artificial intelligence (AI) has emerged as a double-edged sword, especially in the realm of cybersecurity. As we delve deeper into the digital age, the line between AI as a savior and a threat in cybersecurity becomes increasingly blurred. This article explores how AI is reshaping cybersecurity, highlighting both its protective capabilities and the risks it introduces.

### AI as the Savior in Cybersecurity

The role of AI as a protector in cybersecurity cannot be overstated. As cyber threats become more sophisticated, traditional security measures struggle to keep pace. Here, AI steps in as a powerful ally. By leveraging machine learning algorithms, AI systems can analyze patterns and predict potential threats at speeds and accuracies far beyond human capabilities.

One of the most significant advantages of AI in cybersecurity is its ability to learn from data. Security systems powered by AI continuously evolve based on new information, adapting to new threats as they emerge. This dynamic approach is crucial in combating modern cyber-attacks, which are increasingly automated and complex.

For instance, AI can detect anomalies in network traffic that may indicate a breach. Unlike static, rule-based systems, AI-driven tools can discern between benign anomalies and genuine threats, reducing false positives and enabling security teams to focus on actual risks. Moreover, AI can automate responses to detected threats, instantly isolating affected systems and preventing the spread of malware.

### AI as a Threat to Cybersecurity

However, the integration of AI into cybersecurity is not without risks. The very technologies that empower defenders also offer potent tools to attackers. AI can be used to develop malware that learns and adapts to bypass AI-driven security measures. For example, attackers use AI to automate the creation of phishing emails that are increasingly convincing, bypassing traditional spam filters and fooling recipients more effectively. Another significant concern is the potential for AI systems to be compromised. If attackers can manipulate the data used to train AI models (a technique known as "poisoning"), they can cause the system to make incorrect decisions. This vulnerability not only undermines the reliability of AI in security systems but can also turn protective systems into threats themselves.

### Balancing Act: Harnessing AI Responsibility

To maximize the benefits of AI in cybersecurity while minimizing its risks, a balanced approach is necessary. Organizations must invest in robust AI systems while also implementing safeguards to protect these systems from misuse. Regular audits and updates to AI models can help ensure they remain secure and effective against evolving threats. Moreover, collaboration within the cybersecurity community can enhance collective security. Sharing insights and strategies about the use of AI can help create standards and practices that improve security for all, while also addressing ethical concerns.

### Conclusion

AI holds tremendous promise in the field of cybersecurity, offering unparalleled efficiency, accuracy, and adaptability. However, it also presents new challenges and vulnerabilities that must be managed with careful consideration. By understanding and addressing these dual aspects, we can harness AI not just as a savior but also mitigate its potential as a threat, ensuring a safer digital future for everyone.



## GDPR and Beyond: How Compliance is Changing Cybersecurity Strategies?

**Gil Ohayon**  
CISO at Artlist

In May 2018, the General Data Protection Regulation (GDPR) introduced by the European Union marked a significant shift in the global approach to data privacy and security. It set a new standard for privacy rights, security, and compliance, impacting organizations worldwide. This pivotal regulation, along with other global compliance frameworks that have emerged since, has significantly shaped modern cybersecurity strategies.

### GDPR's Impact on Cybersecurity

The GDPR not only mandates how organizations should protect personal data but also enforces substantial penalties for non-compliance. This has prompted companies across industries to reassess and often revamp their cybersecurity architectures. One of the primary mandates of the GDPR is the requirement for organizations to implement "appropriate technical and organizational measures" to secure personal data. This vague yet expansive directive has led to a surge in cybersecurity investments.

Organizations are now more committed than ever to maintaining robust encryption practices, conducting regular vulnerability assessments, and implementing stringent access controls. Moreover, GDPR introduced concepts like

'privacy by design' and 'data protection impact assessments,' which have become integral parts of cybersecurity strategies. These practices ensure that privacy and security considerations are embedded within the developmental phase of projects, rather than as afterthoughts.

### Compliance Beyond GDPR

While GDPR has been a frontrunner in shaping data protection laws, other regions and sectors have developed their regulations that similarly impact cybersecurity strategies. The California Consumer Privacy Act (CCPA) in the United States, for instance, has pushed many American companies to align their data protection standards with those required under GDPR. Similarly, the Brazilian General Data Protection Law (LGPD) and China's Personal Information Protection Law (PIPL) have introduced additional layers of complexity to the compliance landscape.

As organizations aim to comply with multiple, often overlapping regulatory frameworks, cybersecurity strategies have had to become more adaptable and internationally aware. This need has accelerated the adoption of unified compliance frameworks that can cater to multiple regulations simultaneously,

reducing redundancy and ensuring a more streamlined approach to cybersecurity.

### The Future of Compliance and Cybersecurity

As digital transformation accelerates and the global data landscape continues to evolve, compliance will undoubtedly continue to shape cybersecurity strategies. Future regulations will likely address emerging technologies such as artificial intelligence and machine learning, adding more layers to the already complex compliance landscape. Organizations that anticipate and prepare for these changes by integrating compliance deeply into their cybersecurity strategies will not only protect themselves against threats but will also navigate the future more successfully.

In conclusion, GDPR and subsequent regulations have profoundly impacted how organizations approach cybersecurity. Compliance is no longer just a legal obligation; it is a strategic imperative that shapes cybersecurity frameworks, drives technology adoption, and enhances business integrity and trust. As we move beyond GDPR, the intertwining of compliance and cybersecurity will only grow, reinforcing the need for a proactive, integrated approach to both.

# PowerShell Automation and Scripting for Cybersecurity



# Practical Cybersecurity Architecture - Second Edition

## Book Description

After refreshing your knowledge of PowerShell basics and scripting fundamentals, you'll explore PowerShell Remoting and other remote management technologies. You'll learn how to set up and analyze Windows event logs, focusing on the key logs and IDs essential for monitoring your environment. You'll delve into PowerShell's ability to interface with the system, Active Directory, and Azure AD. Additionally, you'll examine Windows internals, including APIs and WMI, and discover methods for running PowerShell without powershell.exe. You'll investigate authentication protocols, enumeration, credential theft, and exploitation to better secure your environment. This includes a practical guide for red and blue teams on everyday security tasks. Lastly, you'll explore various mitigations such as Just Enough Administration, AMSI, application control, and code signing, concentrating on configuration, risks, exploitation, bypasses, and best practices.

## Target Audience

This book is designed for security professionals, penetration testers, system administrators, and red and blue teams interested in utilizing PowerShell for security operations. Readers should have a foundational knowledge of PowerShell, cybersecurity principles, and scripting. Additionally, a basic familiarity with Active Directory, C++/C#, and assembly language will be advantageous for certain sections.

## Where to buy?

You can purchase this excellent book at the O'Reilly website by following the link below [PowerShell Automation and Scripting for Cybersecurity \(oreilly.com\)](https://oreilly.com)

## PowerShell Automation and Scripting for Cybersecurity

**By:** Miriam C. Wiesner  
**Publishing:** Packt Publishing  
**Release Day:** August 2023

## Key Features

- Utilize PowerShell, its mitigation strategies, and enhance attack detection.
- Strengthen your systems and environment against security threats.
- Gain special knowledge about event logs and IDs concerning PowerShell to improve attack detection.
- Set up PSRemoting and understand the associated risks, bypass methods, and best practices.
- Employ PowerShell for system access, exploitation, and hijacking techniques.
- Learn about Active Directory and Azure AD security from both red and blue team perspectives.
- Investigate PowerShell security tactics for dealing with attacks beyond basic commands.
- Explore Just Enough Administration (JEA) to limit executable commands.

## Practical Cybersecurity Architecture - Second Edition

**By:** Diana Kelley, Ed Moyle  
**Publishing:** Packt Publishing  
**Release Day:** November 2023

## Key Features

- Comprehend the architect's role in effectively developing sophisticated security infrastructures.
- Master techniques for drafting architectural documentation, involving stakeholders, and executing designs.
- Learn to enhance and adapt architectural methodologies to address business challenges.
- Buying the print or Kindle version of the book also grants access to a complimentary PDF eBook.

## Book Description

In this book, you will explore the essential principles of cybersecurity architecture as a pragmatic field. These principles are timeless techniques that, once learned, can be applied and adapted to accommodate new and evolving technologies such as artificial intelligence and machine learning. You will discover how to identify and mitigate risks, design secure solutions in a deliberate and consistent manner, communicate security plans effectively, and realize these designs. This latest edition presents strategies for collaborating with implementation teams to turn your security vision into reality, along with methods to ensure your designs remain relevant over time. Throughout your reading, you'll also learn about established frameworks for crafting sturdy designs and strategies to guide the creation of your own security architectures.

## Target Audience

This book serves both new and experienced cybersecurity architects who wish to refine their skills in cybersecurity architecture. It is also beneficial for anyone involved in the planning, implementation, operation, or maintenance of cybersecurity within an organization. Security practitioners, systems auditors, and, to a lesser extent, software developers committed to maintaining organizational security will find this book an invaluable reference guide.

## Where to buy?

You can purchase this excellent book at the O'Reilly website by following the link below: [Practical Cybersecurity Architecture - Second Edition \(oreilly.com\)](https://oreilly.com)

# The right partner for dealing with a complex world of standards and regulations!



A leading consulting company that delivers excellent results.

It takes dedication, expertise, collaboration, and curiosity to help organizations succeed in today's complex regulatory world.

Many thanks to our valued partners and committed customers for making TSG as excellent as we are today!