



Conf42 Incident Management | October 2024

HOW WE REDUCED COSTS BY MILLIONS WITH STRATEGIC SECURITY INITIATIVES

by *Mikhail Baranov*



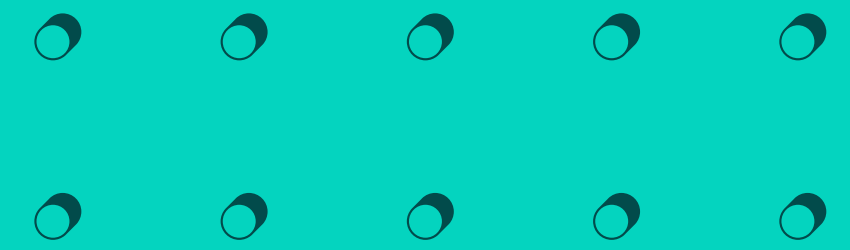


SPEAKER INFO

My name is Mikhail. With over a decade of experience in cybersecurity, I've led the design and implementation of global security infrastructures that have protected financial transactions exceeding \$500 million annually. My initiatives, such as automating compliance checks and establishing a Security Operations Center from scratch, have reduced cybersecurity risks by up to 45% and saved organizations millions in potential losses. My expertise in developing custom solutions, like advanced bot mitigation and secure code reviews, has consistently enhanced security and operational efficiency across international enterprises.

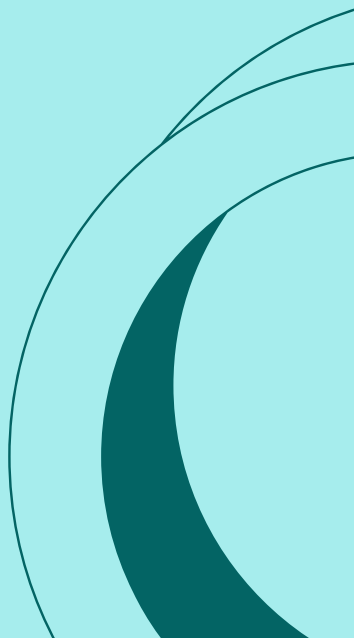


TODAY'S AGENDA



OVER THE PAST FEW YEARS, I'VE HAD THE PRIVILEGE OF LEADING A TRANSFORMATIVE CYBERSECURITY INITIATIVE THAT NOT ONLY FORTIFIED OUR DEFENSES BUT ALSO RESULTED IN SUBSTANTIAL FINANCIAL SAVINGS FOR OUR COMPANY.

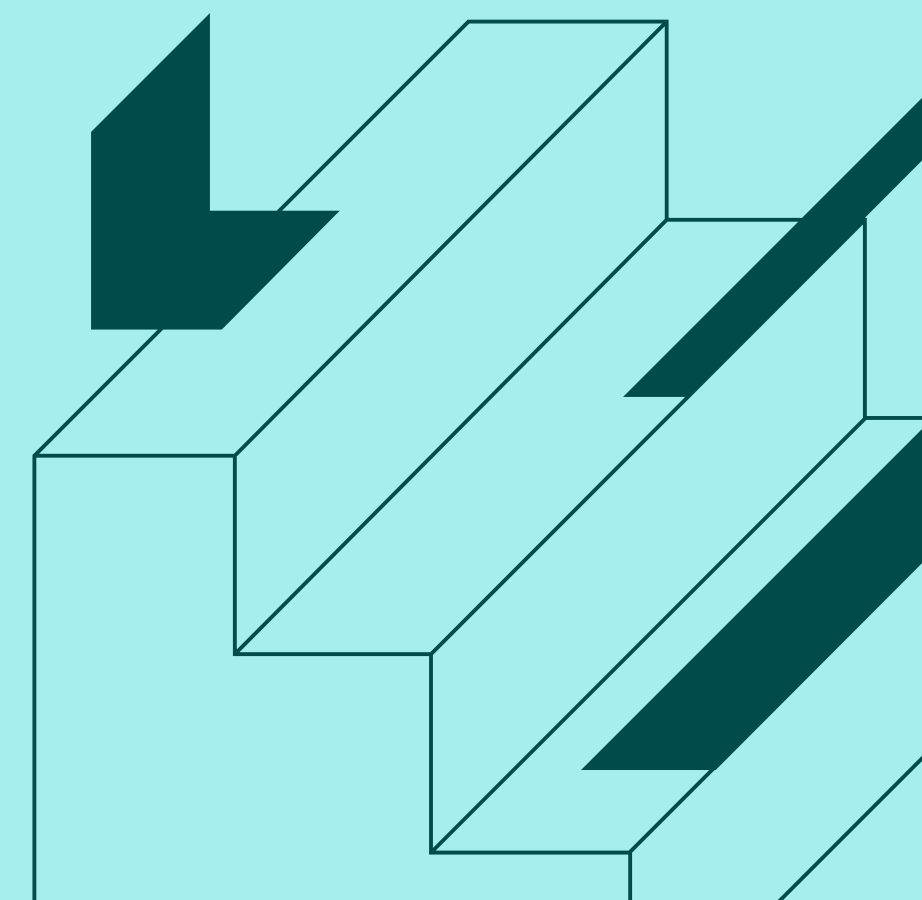
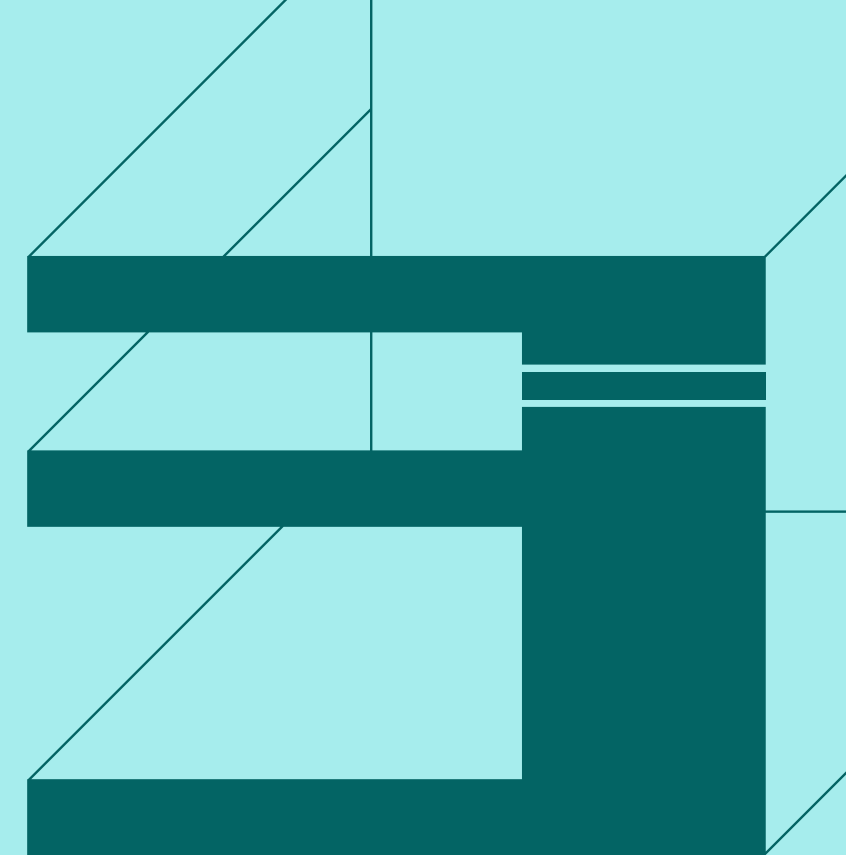
TODAY, I'D LIKE TO SHARE WITH YOU THE JOURNEY WE UNDERTOOK, THE CHALLENGES WE FACED, THE STRATEGIES WE IMPLEMENTED, AND THE INSIGHTS WE GAINED ALONG THE WAY.



When I first joined the Company, it was clear that the organization was at an important turning point regarding its cybersecurity posture.

As a global financial institution handling billions of dollars in transactions annually, we were acutely aware of the increasing sophistication of cyber threats targeting the financial sector. Cybercriminals were no longer lone hackers but organized groups employing advanced persistent threats (APTs), zero-day exploits, and even state-sponsored attacks.

Our existing cybersecurity framework was not consistent enough and some of aspects were ready to counter modern security threats. This lack of a consistent unified approach not only created operational inefficiencies but also left us vulnerable to sophisticated attacks that could exploit these disparities.



The risk was enormous: potential financial losses exceeding \$500 million annually due to data breaches, system downtime, and non-compliance penalties. Moreover, the threat of losing client trust and market share loomed large.

Recognizing the urgency, we embarked on a comprehensive project to overhaul our cybersecurity infrastructure. Our goal was clear: design and implement a unified, resilient cybersecurity framework that would safeguard our global financial operations and ensure strict adherence to international security standards such as SWIFT and PCI DSS.

Identifying Vulnerabilities and Risks

The first step in our journey was to gain a deep understanding of our current security posture. We conducted a thorough risk assessment, which involved several key activities.



RISK ASSESSMENT

Step 1 ----- Network Vulnerability Scanning

Step 2 ----- Penetration Testing

Step 3 ----- Security Configuration Audits

Step 4 ----- Application Security Testing

Step 5 ----- Employee Security Awareness Evaluation

NETWORK VULNERABILITY SCANNING

We used advanced vulnerability scanning tools like Qualys and Acunetix to perform extensive scans of our infrastructure. These tools helped us identify weaknesses such as unpatched software, open ports, and outdated encryption protocols. The results were eye-opening. We discovered over 1,200 vulnerabilities, with several categorized as critical. For instance, we found systems running outdated versions of operating systems that were no longer supported, leaving them susceptible to known exploits.

PENETRATION TESTING

To validate the vulnerabilities identified, we conducted penetration testing using tools like Metasploit, Burp, KaliLinux and manual testing techniques. Our AppSec simulated attacks to exploit the vulnerabilities, gaining unauthorized access to sensitive data and critical systems. In one scenario, we exploited an absence of authorization for requests to our financial transaction systems leading to data exposure and manipulations. This exercise highlighted the potential for a malicious actor to cause significant damage.

SECURITY CONFIGURATION AUDITS


We performed detailed audits of our security configurations, including firewalls, servers, endpoints. We found inconsistencies in firewall rules across different regions, with some allowing unnecessary inbound and outbound traffic. These misconfigurations could have allowed attackers to infiltrate our network or exfiltrate data without detection.

APPLICATION SECURITY TESTING

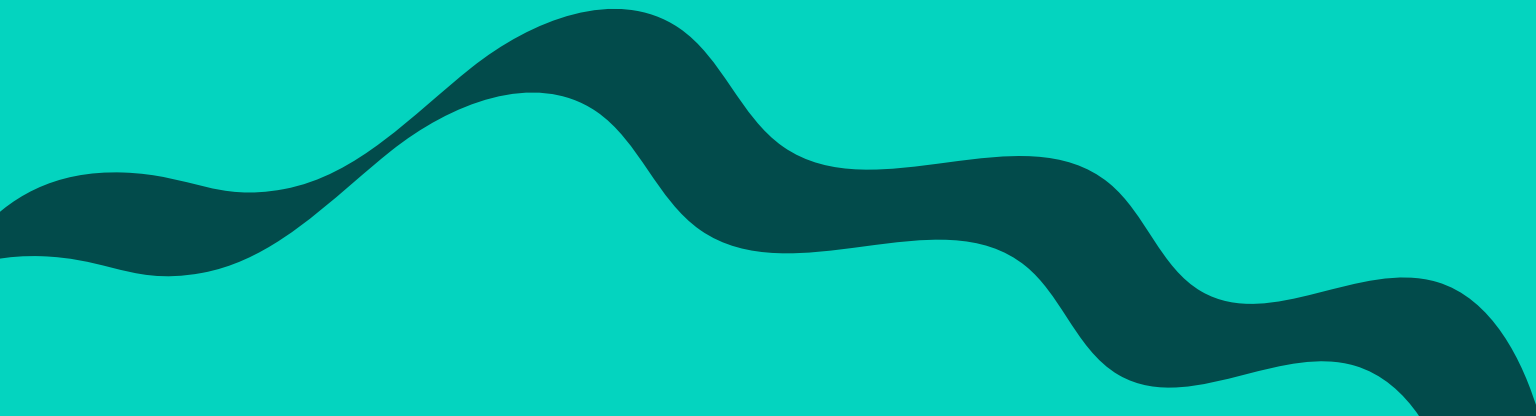
Our internally developed applications were subjected to rigorous security testing using both static and dynamic analysis tools like OWASP ZAP. We uncovered vulnerabilities such as cross-site scripting (XSS), and insecure API endpoints. For example, an application used for client onboarding lacked proper input validation.

EMPLOYEE SECURITY AWARENESS EVALUATION

Understanding that human error is often the weakest link in cybersecurity, we conducted phishing simulations to assess employee susceptibility to social engineering attacks. The results were concerning: 35% of employees clicked on phishing links, and 10% provided their login credentials on fake login pages. This underscored the need for enhanced security awareness training.



We needed to present these findings in a way that would resonate with executive leadership. By quantifying the risks in financial terms, we illustrated the potential impact:



QUANTIFYING THE RISKS

FINANCIAL EXPOSURE

Potential losses exceeding \$500 million annually due to breaches, fraud, and downtime.

REGULATORY PENALTIES

Non-compliance with standards like SWIFT and PCI DSS could result in fines up to \$50 million.

REPUTATIONAL DAMAGE

Loss of client trust could lead to a 15% decrease in market share, equating to hundreds of millions in lost revenue.



STRATEGIC CYBERSECURITY INITIATIVES

Armed with this information, we developed a comprehensive cybersecurity strategy focusing on several key areas.

NETWORK SEGMENTATION AND MICROSEGMENTATION

NETWORK SEGMENTATION

We divided the network into separate segments based on function and sensitivity using VLANs and subnets. This approach limited the spread of potential attacks across the network.

MICROSEGMENTATION

Using software-defined networking (SDN) technologies like Illumio, we enforced granular security policies at the workload level. Each application and service was isolated, and communication was strictly controlled.

This strategy adhered to the zero-trust model, where no network traffic is trusted by default, and every communication is authenticated and authorized.

ADVANCED THREAT DETECTION WITH AI AND MACHINE LEARNING

To stay ahead of sophisticated threats, we integrated artificial intelligence and machine learning into our security operations:

Security Information and Event Management (SIEM): We deployed advanced SIEM solutions ELK and Darktrace, enhanced with machine learning toolkits, to analyze vast amounts of log data in real-time. This allowed us to detect anomalies and potential threats that traditional systems might miss.

User and Entity Behavior Analytics (UEBA): By establishing baseline behavior patterns for users and devices, we could identify deviations indicative of malicious activity. For example, if an employee's account suddenly started accessing large volumes of data at unusual hours, the system would flag this for investigation.

ENDPOINT DETECTION AND RESPONSE (EDR)

Recognizing that endpoints are common entry points for attackers, we:
Deployed EDR Solutions: Tools like EDR were installed on all endpoints with integration with our SIEM, providing real-time monitoring and automated responses to threats.

Automated Isolation: If an endpoint exhibited suspicious behavior, it could be automatically isolated from the network to prevent the spread of malware.

IDENTITY AND ACCESS MANAGEMENT (IAM)

To strengthen access controls:

Multi-Factor Authentication (MFA): Implemented across all critical systems to add an extra layer of security beyond passwords.

Role-Based Access Control (RBAC): Ensured that employees had access only to the resources necessary for their roles, minimizing the risk of unauthorized access. We've completely reengineered the processes for access provisioning and access control to avoid privilege creep and excessive permissions.

SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE (SOAR)

We embraced automation to enhance efficiency:

Automated Incident Response: Using SOAR platforms, we automated responses to common security incidents. As example we've created several scripts for containment after triggers on endpoints and servers.

Playbooks: Developed standardized procedures for handling different types of incidents, ensuring a consistent and swift response based on MITRE matrix.

COMPLIANCE AND STANDARDIZATION

To address the inconsistencies across regions:

Policy Standardization: We created a centralized security policy management system. All regions were required to adhere to the same security standards, reducing gaps in our defenses.

International Standards Compliance: Aligned our controls with frameworks like ISO 27001 and SWIFT's Customer Security Programme (CSP). This not only improved security but also simplified compliance reporting.

EMPLOYEE TRAINING AND AWARENESS

Understanding the importance of the human element:

Mandatory Training Programs: Launched comprehensive cybersecurity training for all employees, covering topics like phishing, social engineering, and secure password practices.

Regular Simulations: Conducted ongoing phishing simulations and provided immediate feedback. Over time, this reduced the click rate on phishing emails from 35% to just 5%.

CASE STUDIES AND SUCCESSES

CASE STUDY 1: THWARTING AN ADVANCED PERSISTENT THREAT

An APT group targeted our organization, attempting to infiltrate our network through spear-phishing emails containing malicious attachments exploiting zero-day vulnerabilities.

Detection: Our AI-powered SIEM detected unusual email patterns and flagged them for investigation.

Response: Automated SOAR playbooks quarantined the suspicious emails and alerted the security team.

Outcome: We neutralized the threat before any damage occurred, preventing potential losses.

CASE STUDY 2: NEUTRALIZING A RANSOMWARE THREAT

An employee inadvertently downloaded ransomware that attempted to encrypt network shares.

Detection: EDR systems identified abnormal file encryption activities.

Response: The infected endpoint was automatically isolated, and files were restored from secure backups stored in WORM (Write Once Read Many) storage.

Outcome: Zero data loss and no ransom paid, saving approximately \$5 million in potential costs.

THROUGH THESE EXPERIENCES, WE GAINED VALUABLE INSIGHTS:

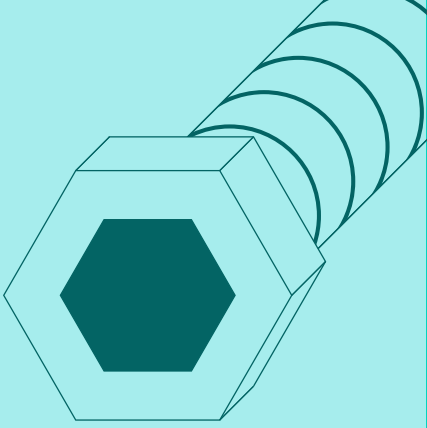
**Proactive Risk
Management is
Essential**

**Automation
Enhances
Efficiency**

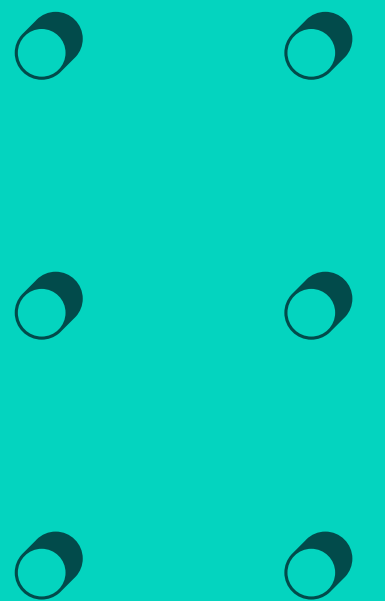
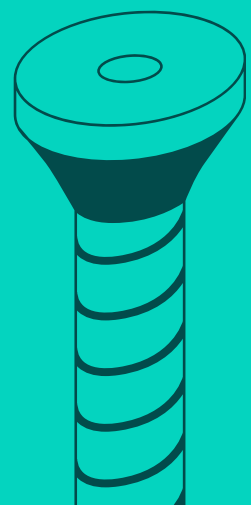
**Standardization
Reduces
Vulnerabilitie**

**Aligning Security
with Business
Goals**

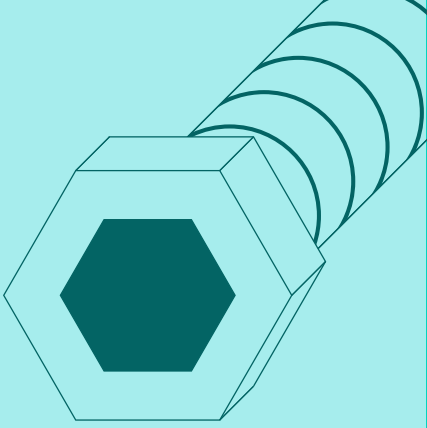
PROACTIVE RISK MANAGEMENT IS ESSENTIAL



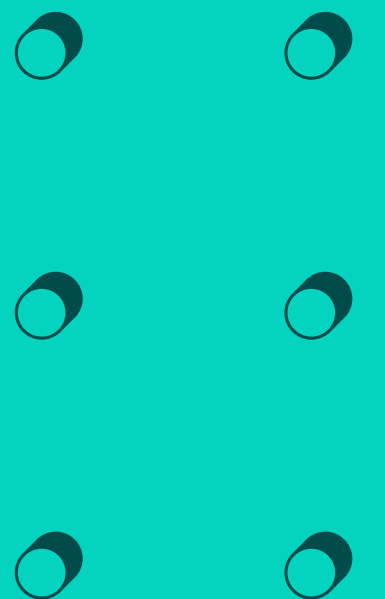
Regular risk assessments and continuous monitoring are critical. By being proactive, we can identify and address vulnerabilities before they are exploited.



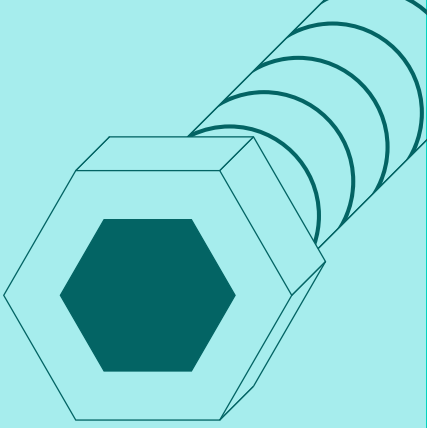
AUTOMATION ENHANCES EFFICIENCY



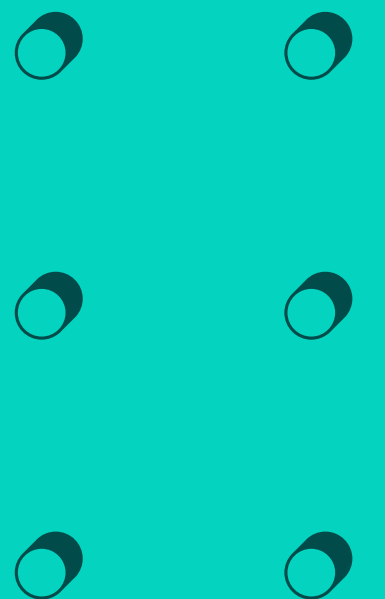
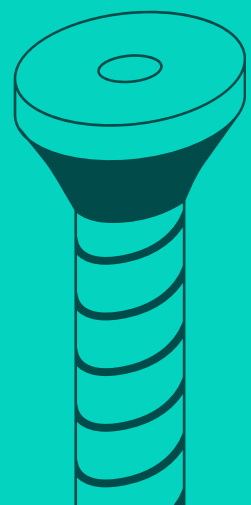
Automation doesn't replace human expertise but enhances it. By automating routine tasks, our security team can focus on more complex threats and strategic initiatives.



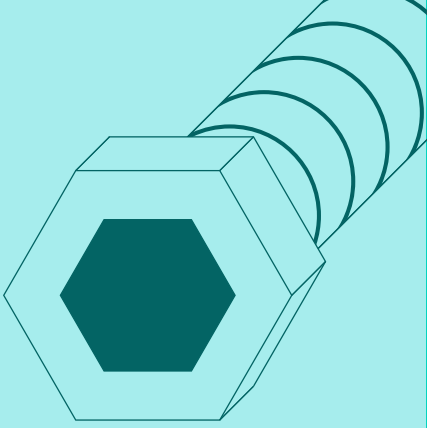
STANDARDIZATION REDUCES VULNERABILITIES



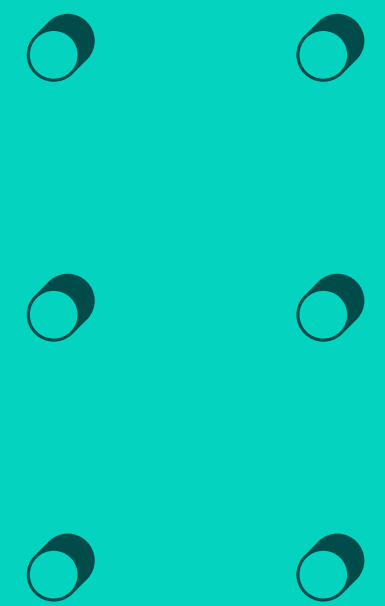
Consistent security practices across all regions eliminate gaps that attackers could exploit. It also simplifies compliance efforts and audits.



ALIGNING SECURITY WITH BUSINESS GOALS



Security initiatives should support business objectives. By demonstrating how security enhances customer trust and protects revenue, we gain support from leadership and stakeholders.



FINANCIAL IMPACT

OUR CYBERSECURITY INITIATIVES HAD A PROFOUND FINANCIAL IMPACT:

- **AVOIDED LOSSES:** OVER \$90 MILLION SAVED BY PREVENTING BREACHES, FINES, AND OPERATIONAL DISRUPTIONS.
- **OPERATIONAL SAVINGS:** REDUCED INCIDENT RESPONSE COSTS BY \$8 MILLION ANNUALLY THROUGH AUTOMATION AND IMPROVED EFFICIENCY.
- **DOWNTIME REDUCTION:** IMPROVED RECOVERY TIMES SAVED \$10 MILLION PER YEAR BY MINIMIZING SERVICE INTERRUPTIONS.
- **RETURN ON INVESTMENT:** ACHIEVED AN ROI OF 150% ON CYBERSECURITY INVESTMENTS WITHIN TWO YEARS.



OUR EFFORTS ALSO BOLSTERED OUR REPUTATION:

Certifications and Compliance: Obtained ISO 27001 certification and complied with SWIFT CSP, enhancing our credibility.

Customer Retention: Strengthened client confidence led to a 7% increase in customer retention, contributing to revenue growth.

RECOMMENDATIONS FOR IMPLEMENTATION

INVEST IN ADVANCED TECHNOLOGIES

Leverage AI and machine learning to enhance threat detection and response capabilities. These technologies can process vast amounts of data and identify patterns that humans might miss.

IMPLEMENT LAYERED SECURITY

Adopt a defense-in-depth strategy. Use multiple security measures at different layers to protect against various types of threats.

STANDARDIZE SECURITY PROTOCOLS

Ensure that security policies and procedures are consistent across all regions and departments. This reduces vulnerabilities and simplifies compliance.

RECOMMENDATIONS FOR IMPLEMENTATION

FOSTER A SECURITY-CONSCIOUS CULTURE

Invest in regular training and awareness programs. Empower employees to be the first line of defense against cyber threats.

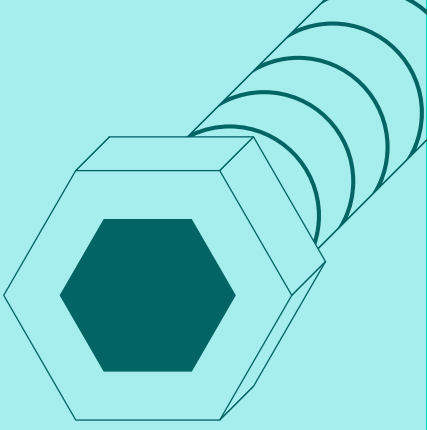
ALIGN SECURITY WITH BUSINESS STRATEGY

Communicate the value of cybersecurity in business terms. Demonstrate how security initiatives protect revenue, enhance customer trust, and support growth.

CONCLUSION

In today's interconnected world, cybersecurity is not just a technical issue but a fundamental business concern. Our journey demonstrates that with a strategic approach, it's possible to significantly reduce risks and achieve substantial financial savings. By identifying vulnerabilities, implementing advanced security measures, and fostering a culture of security awareness, we protected our assets and supported our company's growth.

I hope our experiences provide valuable insights that you can apply within your own organizations. Cybersecurity is a continuous journey, and staying ahead of evolving threats requires commitment, innovation, and collaboration.



What are your thoughts about the conference today? I'm happy to answer any questions you may have.

**THANK YOU
FOR YOUR ATTENTION!**

