Defense in Depth: Financial Services Regulatory Pressures

2025 Cyber Symposium

forvis mazars

Agenda

1. Introductions
2. Current Cyberthreat Landscape
3. What Is Defense in Depth?
4. Building the Layers
5. The Role of Comprehensive Testing
6. Recommendations & Takeaways

Introductions

IT Risk & Compliance

Todd Hjerpe

Managing Director

Ray Baxter

Director

Justin Lance

Senior Manager

Current Cyberthreat Landscape

forvis mazars

THE IMPACT OF CYBERATTACKS

Cyberattacks in the **Financial Services Sector** tended to see costs accrue in later years following the breach. An average of 24% of cyberattack costs was accrued more than two years after the attack occurred with the average cost being $6.08 million. *

Financial Losses.

Reputational Damage.

Legal & Regulatory Consequences.

Operational Disruptions.

"There are only two types of companies in the world: those that have been breached & know it & those that have been breached & don't know it." – Ted Schlein (CEO of Fortify Software + many more)

forvis mazars

*Source: 2024 IBM Cost of a Data Breach Report

COMMON VULNERABILITIES

Cyberattacks exploit various vulnerabilities in systems, networks, & practices to gain unauthorized access, extract sensitive information, or disrupt services. The Financial Services Sector is a prime target for cyberattacks due to the sensitive nature of the data it handles & the potential financial gain for attackers.

- Human Error/Social Engineering.
- Weak Authentication Mechanisms.
- Outdated Software & Systems.
- Misconfigured Security Configurations.

Core Concept: What Is Defense in Depth

DEFENSE IN DEPTH

Cybersecurity defense in depth is a critical strategy for protecting sensitive information & systems from increasingly sophisticated cyberthreats. This approach involves implementing multiple layers of security controls & measures, each designed to address different aspects of the cyber kill chain. By combining various defensive mechanisms, such as firewalls, intrusion detection systems, encryption, & user training, organizations can create a robust security posture that is more resilient to attacks.

Defense in depth helps ensure that even if one layer is compromised, additional layers provide continued protection, reducing the likelihood of a successful breach. This comprehensive strategy not only safeguards valuable data but also helps enhance overall trust & confidence in an organization’s ability to manage & mitigate cyber risks.

DEFENSE IN DEPTH TACTICS

It is critical to understand that, while there is no silver bullet, cybersecurity solution & technology, a comprehensive cybersecurity strategy, implements defense in depth with multiple layers of security controls & measures to protect data & resources. By integrating these layers, financial institutions can better protect themselves against a wide range of threats.

- **Patch Management.**
  Track & apply updates to operating systems, software, & hardware.
- **Intrusion Detection & Prevention Systems.**
  Use tools to detect malicious network traffic & provide alerts.
- **Endpoint Detection & Response.**
  Logging & active monitoring of events throughout each managed system on the network.
- **Multi-Factor Authentication.**
  Use of multiple authentication types (something the user knows, something the user has, or something the user is) to verify a user’s identity.
- **Backup & Restoration Strategy.**
  Maintain secure copies of operational data & systems, & test copies to help ensure completeness & reliability.
- **Centralized Logging & Alerting.**
  Compare ongoing traffic behavior to pre-defined baselines to identify anomalies by collecting & analyzing log data from various sources.

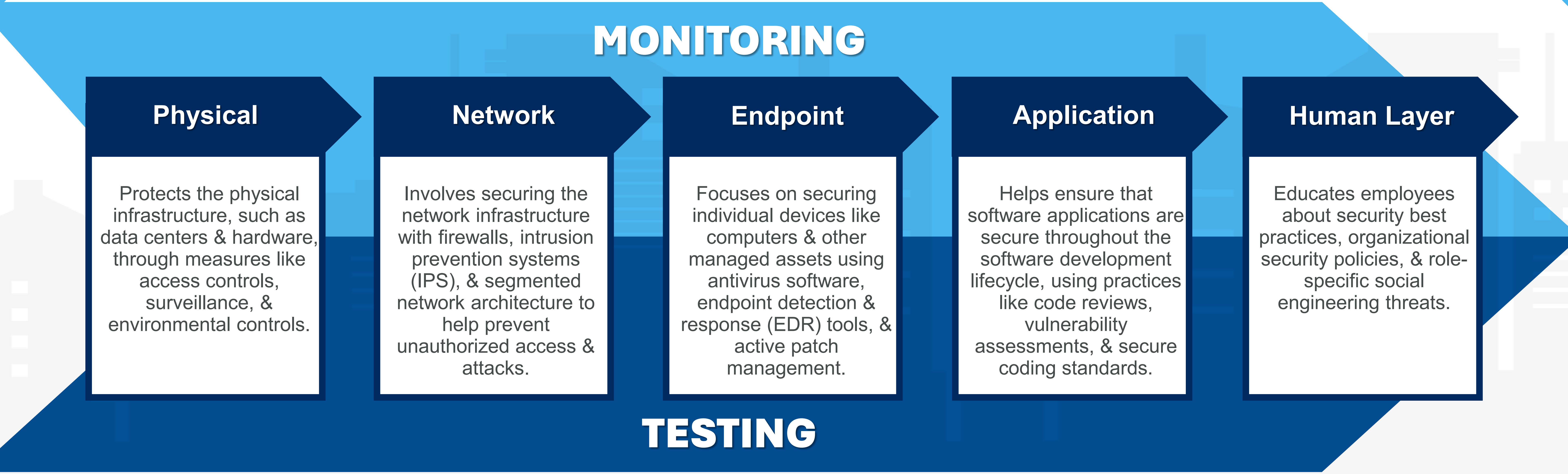
ROLE OF GOVERNMENT REGULATIONS

Defense in depth is an essential cybersecurity strategy in the Financial Services Sector because it provides multiple layers of security controls to protect sensitive financial data, systems, & transactions. Cybersecurity defense in depth is foundational in meeting the Office of the Comptroller of the Currency (OCC), Federal Reserve, & Federal Deposit Insurance Corporation (FDIC) regulatory expectations. The defense in depth strategy aligns with industry & regulator leading frameworks Cyber Risk Institute (CRI) Profile, Federal Financial Institutions Examination Council (FFIEC), & National Institute of Standards & Technology (NIST).

Building the Layers

BUILDING THE LAYERS

Cybersecurity defense in depth is a multilayered approach to security that incorporates various components to help financial institutions protect against a wide range of threats.



MONITORING

Physical

Protects the physical infrastructure, such as data centers & hardware, through measures like access controls, surveillance, & environmental controls.

Network

Involves securing the network infrastructure with firewalls, intrusion prevention systems (IPS), & segmented network architecture to help prevent unauthorized access & attacks.

Endpoint

Focuses on securing individual devices like computers & other managed assets using antivirus software, endpoint detection & response (EDR) tools, & active patch management.

Application

Helps ensure that software applications are secure throughout the software development lifecycle, using practices like code reviews, vulnerability assessments, & secure coding standards.

Human Layer

Educates employees about security best practices, organizational security policies, & role-specific social engineering threats.

TESTING

“There’s no silver bullet solution with cyber security; a layered defense is the only viable defense”
– James Scott (Senior Fellow & co-founder of the Institute for Critical Infrastructure Technology)

forvis mazars

THIRD-PARTY & ECOSYSTEM RISK

Managing third-party & ecosystem cybersecurity risks involves several key practices to ensure the resilience & security of external entities & interconnected networks that an organization relies on.

Risk Assessments

Regularly assess & identify potential risks associated with each critical vendor. Evaluate financial stability, compliance with regulations, cybersecurity measures, & operational resilience.

Monitoring & Auditing

Continuously monitor vendor activities with real-time alerts for suspicious behavior. Conduct regular audits & assessments of vendor security practices, systems, & service level agreements.

Strategic Alignment

Ensure that the vendor's goals & strategies align with your organization's long-term objectives. Consider how the vendor contributes to your competitive advantage & business growth.

forvis mazars

ENHANCING LAYERS WITH EMERGING TRENDS

By incorporating emerging technologies into existing layers, organizations can enhance their overall security posture & adaptability to evolving threats. Continuous advancement & research into emerging technologies are essential to maintain a robust defense posture against the growing sophistication of cyberthreats.

- Artificial intelligence & machine learning in threat detection.
- Blockchain for secure transactions.
- Zero Trust Architecture.

THE FUTURE OF CYBERSECURITY

The future of cybersecurity is rapidly evolving, driven by technological advancements, shifting threat landscapes, & increasing security demands. It is exciting & challenging. As technology evolves, cybersecurity professionals must stay ahead of threats & develop new strategies to protect against emerging risks.

Rise of autonomous security systems.

Autonomous security systems use artificial intelligence (AI), machine learning (ML), & advanced technologies to detect, respond to, & prevent cyberthreats without human intervention.

Increased emphasis on cyber resilience.

Cyber resilience is the ability of an organization to anticipate, prepare for, respond to, & recover from cyberthreats, minimizing the impact on its operations & reputation.

Beyond the Basics: The Role of Comprehensive Testing

forvis mazars

THE ROLE OF COMPREHENSIVE TESTING

Financial institutions must prioritize comprehensive & continuous testing to stay in front of an ever-evolving cyber landscape. Comprehensive testing helps ensure that each phase within a security program is scrutinized, & deficiencies are identified before an attacker exploits them. Continuous testing provides actionable insights to inform security decisions, helping ensure that a security program remains effective & responsive to emerging industry threats.

Penetration Testing

Monitoring Practices

Regulatory Expectations

forvis mazars

CONTINUOUS TESTING & MONITORING

- Ransomware Assessment
- Tabletop Exercise
- Red Teaming
- Penetration Test
- End-User Awareness
- Managed Security Service Provider
- Benchmark Assessment

Continuous testing & monitoring provide actionable insights to inform security decisions, helping ensure that a security program remains effective & responsive to emerging industry threats.

forvis mazars

Recommendations & Takeaways

forvis mazars

KEY RECOMMENDATIONS

A defense in depth approach enhances resilience, adaptability, & overall security posture, protecting sensitive financial data & systems effectively.

Multi - Layered Network Architecture

Dividing a network into multiple layers, each with its own set of security controls & protocols.

Advanced Threat Detection & Response

Comprehensive solution to detect, respond to, & mitigate advanced cyberthreats in real-time

Consistent Testing & Monitoring

Ensure that the defense in depth strategy remains resilient & effective against cyberthreats.

forv/s mazars

KEY TAKEAWAYS

These takeaways underscore the importance of a holistic, layered approach to cybersecurity within the Financial Services Sector, ensuring not only compliance & protection but also the resilience & adaptability necessary to operate securely in a complex threat environment.

Proactive vs. Reactive

Defense in depth emphasizes proactive measures to prevent breaches rather than simply reacting to them after they occur.

Holistic Approach

Security must be integrated throughout the organization at every level, involving people, processes, & technologies.

Evolving Threat Landscape

The Financial Services Sector must continually adapt & evolve its defense mechanisms to address new & emerging cyberthreats.

Collaboration Is Key

Collaboration both within the organization & with external partners, including information sharing groups, can enhance overall cybersecurity resilience.

THANK YOU

FOR YOUR ATTENTION & PARTICIPATION

The Financial Services Sector is a prime target for cyberattacks due to the sensitive nature of the data it handles & the potential financial gain for attackers. Defense in depth is a vital cybersecurity strategy that utilizes multiple, layered security measures to protect sensitive data & systems. This approach ensures that even if one layer is compromised, other layers remain intact to prevent a successful attack.

forvis mazars

Contact

Forvis Mazars

Todd Hjerpe
Managing Director
P: 901.261.4164
todd.hjerpe@us.forvismazars.com

Ray Baxter
Director
P: 629.900.2172
ray.baxter@us.forvismazars.com

Justin Lance
Senior Manager
P: 704.367.7047
justin.lance@us.forvismazars.com

The information set forth in this presentation contains the analysis & conclusions of the author(s) based upon his/her/their research & analysis of industry information & legal authorities. Such analysis & conclusions should not be deemed opinions or conclusions by Forvis Mazars or the author(s) as to any individual situation as situations are fact-specific. The reader should perform their own analysis & form their own conclusions regarding any specific situation. Further, the author(s)' conclusions may be revised without notice with or without changes in industry information & legal authorities.