`

STATE BAR OF WISCONSIN
PINNACLE
Your Practice. Our Purpose.

AMC 2025

WALA Session 1

Cybersecurity for Law Firms: Protecting Client Trust in the Digital Era

Presented By:
David Eichkorn, Elevity, Madison

About the Presenter...

David Eichkorn is a dedicated strategist and IT professional with over 25 years of experience in aligning technology with business goals. For more than half of his career, David served in internal IT leadership roles, giving him firsthand insight into the challenges organizations face as they grow and evolve. In the latter part of his career, he transitioned to supporting clients directly, leveraging his experience to develop and execute technology roadmaps that drive operational efficiency, bolster security postures, and promote long-term success. As a trusted advisor, David works closely with clients to understand their unique needs, crafting tailored solutions that bridge the gap between IT and business outcomes.

.

CYBERSECURITY FOR LAW FIRMS

PROTECTING CLIENT TRUST

elevITy

1

OBJECTIVES

CYBERSECURITY:

- WHAT IS IT?
- WHY IS IT RELEVANT?
- WHAT IS THE IMPACT?
- HOW DO YOU MANAGE RISK?

ACTION PLAN AND NEXT STEPS FOR YOUR PRACTICE

elevITy

2

WHAT IS CYBERSECURITY?

Cybersecurity is the practice of protecting data, systems, networks and programs from digital attacks, unauthorized access, damage or theft.

That's true but it's so much more and needs to be a comprehensive solution that protects businesses information, people, clients, and reputation!

3

HIGH VALUE TARGETS

- **90% of businesses are SMB[1]**
- **SMBs account for 50% of employment[1]**
- **40% of overall economic activity created by SMBs[1]**

1. The 2024 Sophos Threat Report: Cybercrime on Main Street – Sophos News

4

WHY ARE LAW FRIMS ARE A TARGET?

- Often underinvested, underinsured, and underprepared, making them low-hanging fruit for threat actors.
- High "hack-to-leverage" ratio: even a small firm can hold sensitive data for billion-dollar clients.
- Involved in M&A, litigation, and government affairs, making data highly valuable on the dark web or for espionage.

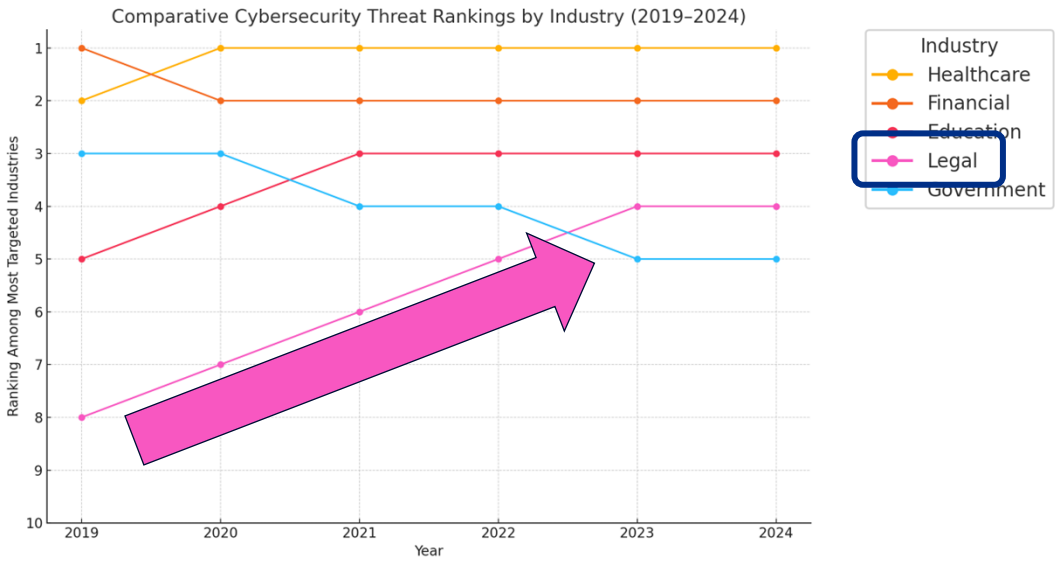
5

KEY POINTS IN LEGAL SECTOR

- 2023-2024 Trends show that law firms were among the top 5 most targeted by organized crime units.
- Small-to-midsize law firms are disproportionately affected due to fewer cybersecurity controls.
- The American Bar Association (ABA) reported in 2023 that 29% of law firms experienced a known cyber breach, and many others likely went undetected or unreported.

6

THREAT RANKINGS BY INDUSTRY



7

RISK IMPACT: LEGAL SECTOR vs. GENERAL SMB

Risk Category	Legal Sector	General SMB
Sensitivity of Data	**Extremely high (privileged info)**	Moderate to high
Regulatory Exposure	High (ABA, HIPAA, GDPR, client contracts)	Variable
Ethical/Professional Risk	Yes (client trust, bar association)	Typically, N/A
Target Value to Attackers	High (legal secrets, VIP clients)	Depends on industry
Reputational Impact	**Severe, long-lasting**	Often localized
Client-Imposed Security	**Increasingly common**	Rarely contractual
Third-Party Risk	High (vendors, experts, co-counsel)	Moderate

elevITy

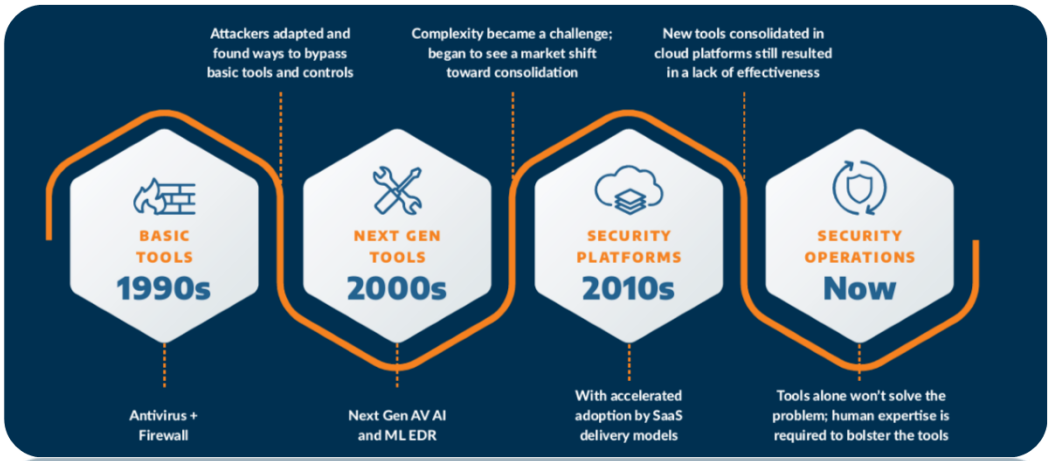
8

WHAT'S AT STAKE?

Client Trust	Firm Integrity	Brand Value
Regulatory Compliance	Professional Reputation	Operational Continuity
Financial Health	Privileged Data	Workplace Culture

9

HISTORY OF CYBER THREATS



10

RISK IMPACT: LEGAL SECTOR vs. GENERAL SMB

Threat Type	Legal Sector Sensitivity	General Risk Level	Notes
Phishing & BEC	**Very High**	High	Especially during real estate or financial transactions
Ransomware	**Very High**	High	Client confidentiality at risk
Insider Threats	High	Medium	Often undetected until damage is done
Supply Chain Attacks	High	Medium	Often indirect but highly impactful
Data Exfiltration/Espionage	**Very High (BigLaw)**	Medium	Often nation-state or corporate espionage
Unpatched Systems	High	High	Many firms lag in patch management
Insecure Remote Access	High	High	Especially post-COVID remote adoption
Credential Attacks	High	Medium	Weak password policies are common

AelevITy

11

SYSTEMS TO PROTECT



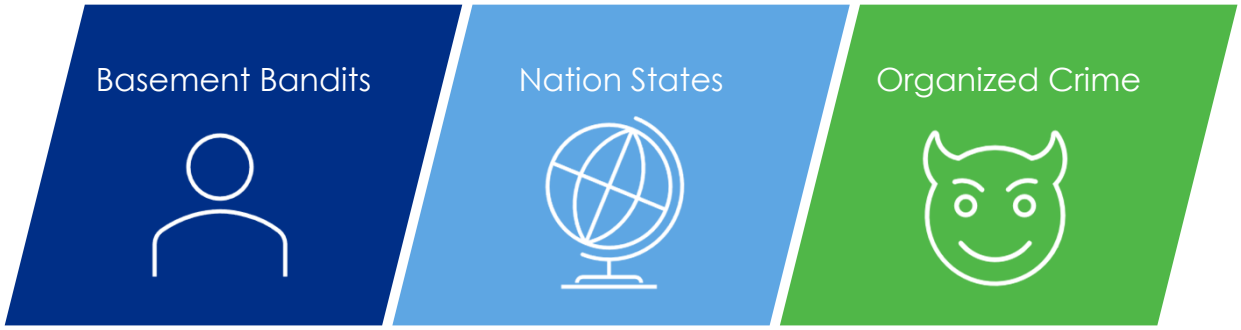





AelevITy

12

BAD ACTORS



Your data is valuable to bad actors, because it's valuable to you!

elevITy

13

GAINING ACCESS

Bad actors work to find access into corporate systems through social engineering and testing, and environment vulnerabilities!

49% **Credentials**

17% **Phishing**

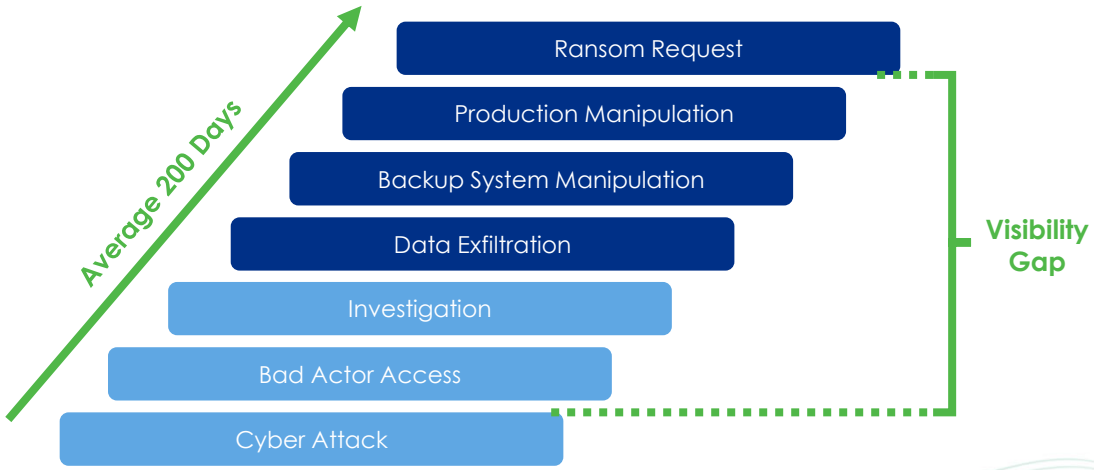
9% **Exploits**

elevITy

*Verizon 2023 DIBR Report

14

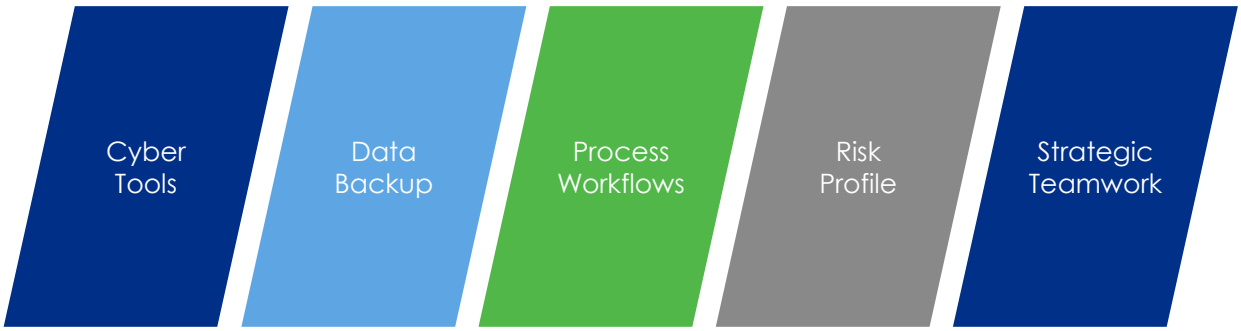
GAINING ACCESS IS JUST THE START



15

MANAGED RISK

A comprehensive strategy includes more than blocking attacks, it includes:



16

LAYERED SECURITY APPROACH

AWARENESS

Arm your team with the knowledge they need to mitigate cybersecurity risk.

DETECTION

Reduce the noise of thousands of security products, get the alerts that matter in real time.

RESPONSE

Rapidly react to emerging threats across your network.

RECOVERY

Timely recovery to normal business operations to avoid costly downtime.

elevITy

17

LAYERED SECURITY APPROACH

91% of breaches start with a phishing email.

AWARENESS

Arm your team with the knowledge they need to mitigate cybersecurity risk.

DETECTION

Reduce the noise of thousands of security products, get the alerts that matter in real time.

RESPONSE

Rapidly react to emerging threats across your network.

RECOVERY

Timely recovery to normal business operations to avoid costly downtime.

elevITy

18

LAYERED SECURITY APPROACH

It takes an average of **206 days** to identify an intrusion.

AWARENESS

Arm your team with the knowledge they need to mitigate cybersecurity risk.

DETECTION

Reduce the noise of thousands of security products, get the alerts that matter in real time.

RESPONSE

Rapidly react to emerging threats across your network.

RECOVERY

Timely recovery to normal business operations to avoid costly downtime.

ElevITy

19

LAYERED SECURITY APPROACH

SIEM/SOC enables Elevity to reduce threat actor dwell time from **months to minutes.**

AWARENESS

Arm your team with the knowledge they need to mitigate cybersecurity risk.

DETECTION

Reduce the noise of thousands of security products, get the alerts that matter in real time.

RESPONSE

Rapidly react to emerging threats across your network.

RECOVERY

Timely recovery to normal business operations to avoid costly downtime.

ElevITy

20

LAYERED SECURITY APPROACH

60% of SMB organizations that fall victim to a data breach close within 6 months.

AWARENESS

Arm your team with the knowledge they need to mitigate cybersecurity risk.

DETECTION

Reduce the noise of thousands of security products, get the alerts that matter in real time.

RESPONSE

Rapidly react to emerging threats across your network.

RECOVERY

Timely recovery to normal business operations to avoid costly downtime.

elevITy

21

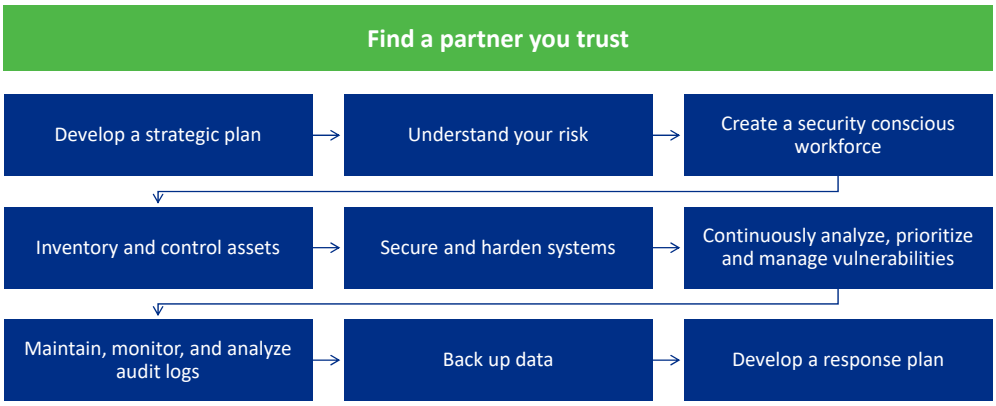
A TECHNOLOGY ROADMAP

- Aligns technology initiatives with your business goals
- Provides focus to prioritize, invest and guide decisions
- Should be frequently updated based on business need
- Includes cybersecurity and business continuity planning
- Provides opportunity using risk and change management
- Delivers results through transparency

elevITy

22

ACTION PLAN



23

THERE IS NO QUICK FIX

- An effective, sustainable, proactive cybersecurity program does not simply involve a one-time effort, nor can be a siloed project.
- A managed risk approach removes much of the fear, uncertainty, and doubt that can plague SMBs.
- You cannot manage risk and protect your organization if you do not know where and in what form it exists.

24

25