IT Solutions

Securing Legal Institutions: Why Cybersecurity Needs To Be a Firm Priority

How a proactive cybersecurity strategy preserves trust, revenue, and brand reputation.

ALA Annual Conference

Are you going to **Nashville** next week for the
ALA Annual Conference?

We'll be there! Come check out our booth and connect with our team! We'd love to see you there!

<u>Booth#1107</u>

ITS

Executive Summary

1 Identity is the new perimeter

Threats continue to shift toward users and their identities as the weakest link.

2 Key Challenges

Firms often lack understanding of risks due to users and data access.

3 Business Resiliency Through Data Protection

Integrated threat detection, zero-trust architecture, and continuous monitoring are crucial.

Legal Org Threat Profile

ITS

Why Would a Threat Actor Want to Target a Legal Org?

Why They Are Targeted

Sensitive Data (PII, PHI, Finance)

Ransomware/Data Theft Extortion

Less Mature Security Posture

Relationships to Exploit

Most Likely Threats

Cyber Criminals

Nation State Adversaries

Supply Chain Attacks

Insider Threats

CURRENT SITUATION

ITS

$10.5 Trillion

Projected damages by threat actors in 2025

558%

Increase in identity-focused attacks since 2023

47%

Of small businesses suffered an attack in the last year

31%

Of clients will terminate the relationship following a data breach

3x

Small businesses are 3 times more likely to be targeted than larger companies

INSIGHTS FROM VERIZONS 2025 DBIR BY THE NUMBERS

ITS

37%
44%
$115,000

Ransomware and Extortion Based Attack Trends

- 37%: Percentage Increase in Ransomware attacks YoY
- 44%: Percentage of data breaches that involve ransomware of some kind
- 115,000: Median cost of a ransom payment (in USD)

88%
22%

SMB Targeting Trends and Credential Abuse

- 88%: Rate that SMBs experience ransomware and extortion related breaches vs large organizations
- 22%: percentage of all breaches using credential theft for initial access

34%

Vulnerability Exploitation Trends

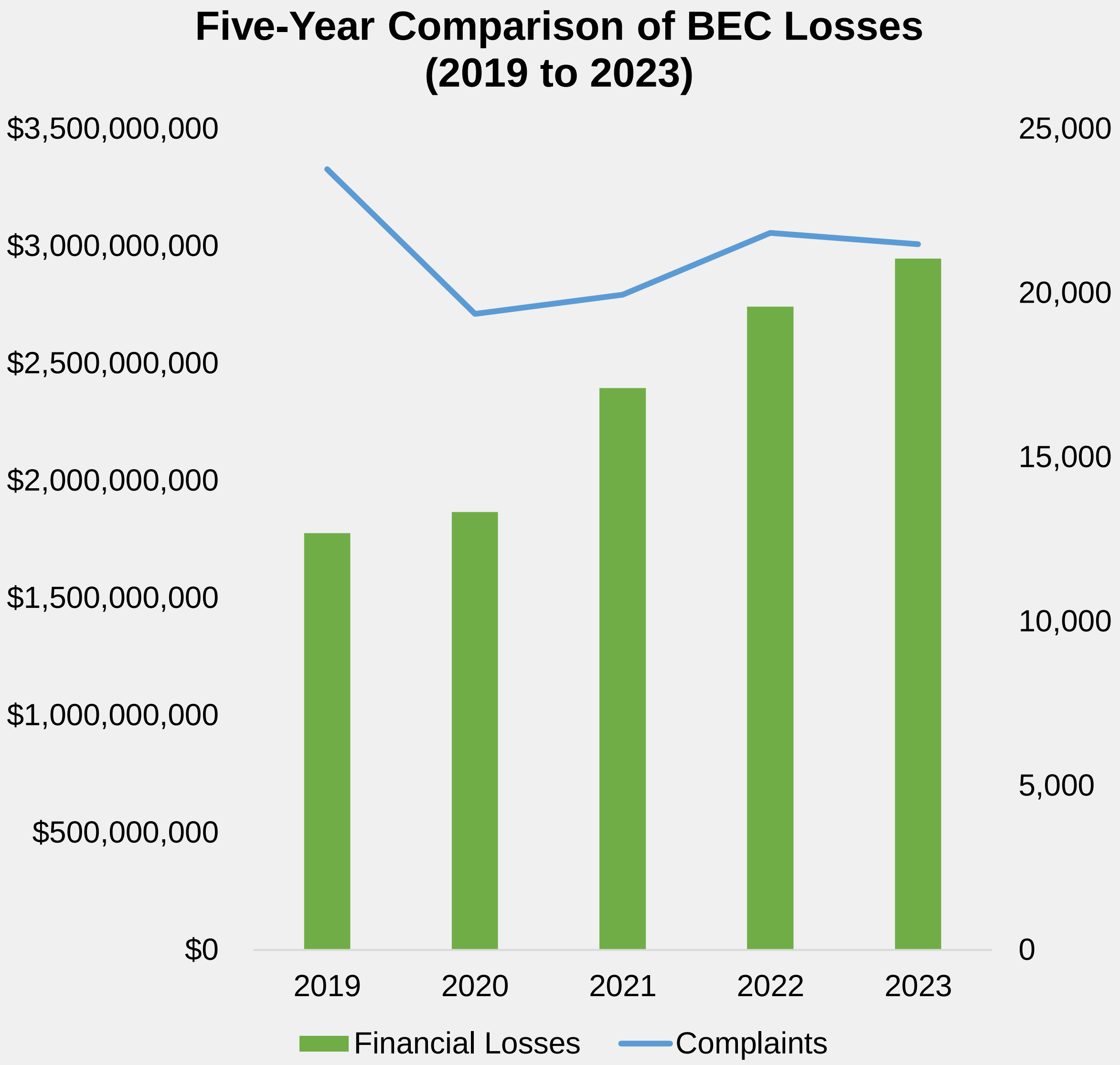
34% increase VPN and perimeter device vulnerability exploitation attacks, incl. Zero Days

ITS

Business Email Compromise Explained

- BEC is one of the most financially damaging online crimes
- Criminals gain access to a legitimate business email to:
  - Fake Invoices
  - Impersonate a Partner
  - Steal Intellectual Property

AI and Criminal Undergrounds Lower Barrier to Entry



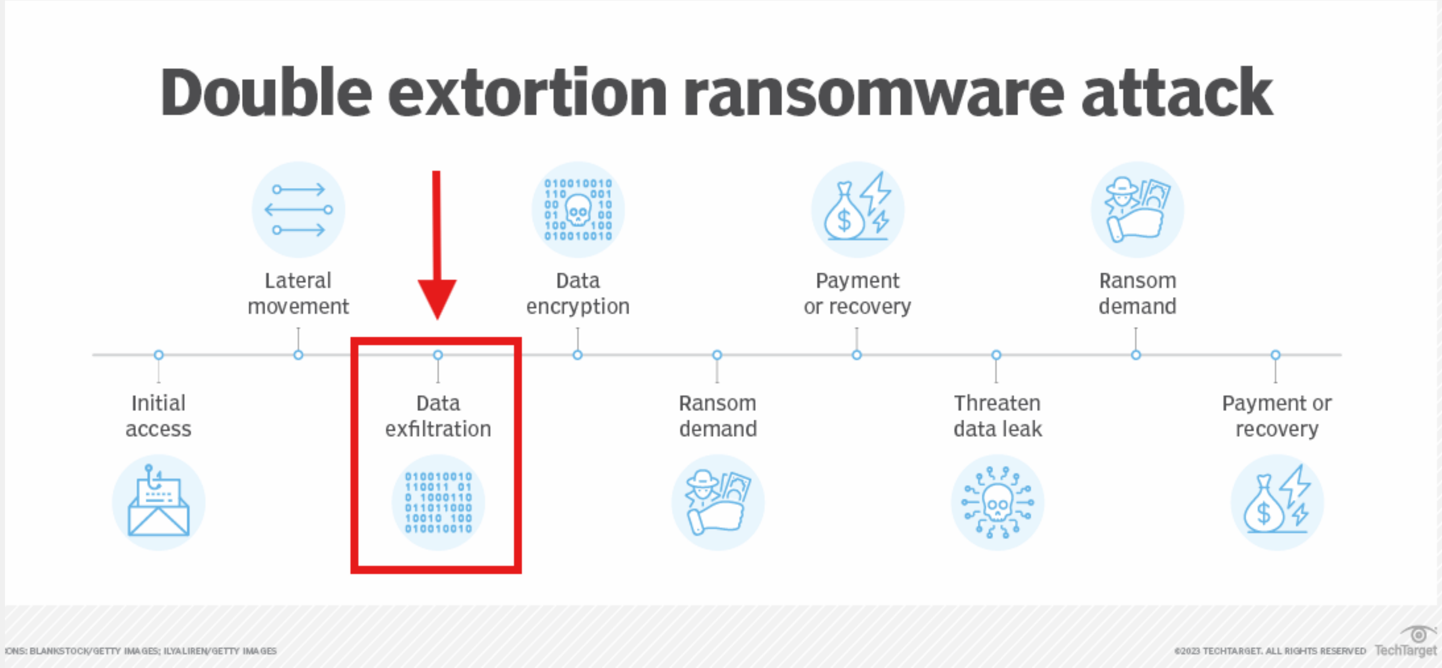
Data source: FBI IC3 Internet Crime Report (2021, 2022, and 2023).

EVOLVING THREAT LANDSCAPE: SHIFTS FROM RANSOMWARE TO DATA THEFT EXTORTION

ITS

Data Theft Extortion (DTE) Explained

- DTE represents the continued shift by threat actors to create pain for victims as defenders are getting
- DTE as the evolution of Ransomware:
    - Adversaries steal sensitive data and threaten to release it unless a ransom is paid
    - Uses legitimate technology solutions and existing capabilities
    - Designed to evade detection of standard endpoint centric defenses



Data source: Techtarget

CYBER RISK IS BUSINESS RISK_

Cyber risk increases risk across every domain.

Managing cyber risk is essential for managing all other types of risk.

STRATEGIC RISK

- Cybersecurity vulnerabilities can derail long-term business strategies.
- Intellectual property theft compromises competitive advantages.
- Major cyber events might force unexpected strategic realignments.

REPUTATIONAL RISK

- Cyber incidents can destroy brand perception and sentiment.
- Customer and vendor confidence diminishes rapidly.
- News stories and word of mouth increase reputational damage.

CYBER RISK

FINANCIAL RISK

- Cyber incidents can drain financial resources through direct theft.
- Unexpected costs from breach investigations and potential fines.
- Customer trust erosion leads to significant revenue losses.

COMPLIANCE RISK

- Non-compliance result in financial penalties & operational restrictions.
- Reporting requirements for cyber incidents are increasingly stringent.

OPERATIONAL RISK

- Cyberattacks can completely halt critical business operations.
- System disruptions interrupt core workflows and communication channels.
- Digital infrastructure becomes vulnerable to widespread technological failure.

LEGAL RISK

- Data breaches can trigger substantial litigation from affected parties.
- Contractual obligations are compromised based on inability to meet requirements.
- Intellectual property protections may be weakened through digital vulnerabilities.

ITS

Consequences of Inaction

Financial Loss

1

Average cost of a data breach in finance can reach millions.

Regulatory Fines & Legal Liability

2

Non-compliance penalties can soar into the millions, alongside potential class-action lawsuits.

Eroded Customer Confidence

3

Loss of trust may impact the ability to retain clients.

Competitive Disadvantage

4

Institutions with weak security might be bypassed by major clients seeking safer partnerships.

AVERAGE COSTS OF DEALING WITH BREACHES

ITS

[redacted]

	Average Costs	High End of Costs
Investigation and Recovery	$77,957	$3,930,000
Fines	$20,623	$655,000
Cost to Reputation	$73,393	$1,310,000
Missed Opportunities	$23,806	$6,550,000
Other Costs	$58,666	$3,275,000

ITS

Key Features of an Effective Security Approach

Integrated Threat Detection & Response

A unified approach that consolidates alerts and speeds incident response.

Zero-Trust Architecture

Restrict access and validate every request to minimize insider and external threats.

Encryption & Data Protection

Safeguard sensitive customer and transaction data end-to-end.

Proactive Hygiene and Systems

Administration

Continuous monitoring, patch management, audits and alignments, data governance.

What Success Looks Like

Reduced Incident Frequency & Severity

Fewer attacks slip through, and those that do are contained quickly.

Audit-Ready at All Times

Avoid last-minute scrambles and demonstrate compliance with confidence.

Improved Competitive Advantage

Investing in security can help increase competitive advantage throughout multiple industries.

Client Trust & Confidentiality Assurance

Demonstrate a strong commitment to protecting sensitive client data, reinforcing client confidence and supporting long-term relationships.

A Proven Plan Increases IT Success

ITS

- ASSESS
- PLAN
- IMPLEMENT
- MANAGE
- OPTIMIZE

It's a lot.
It's not easy.
Let us help.

Q&A

Thank you.

Don’t forget to come see
us in Nashville!

Booth#1107