The Resurgence of Manufacturing: Cyber & Organizational Resilience

Manufacturing Sector

Justin Hill, Ben Owings, Ben Doane | October 2025

Agenda

1. The state of manufacturing: Why resilience matters
2. Cyberthreat landscape & organizational risk
3. Building business continuity & disaster recovery plan
4. Proactive cybersecurity strategies for manufacturers
5. GenAI in security operations: from detection to autonomous SOC
6. Real-world scenarios & best practices

Resurgence of Manufacturing
Cyber & Organizational Resilience

Presenters

Justin Hill

Lead Consultant, CFO & Business Consulting

Ben Owings

Director, IT Risk & Compliance

Ben Doane

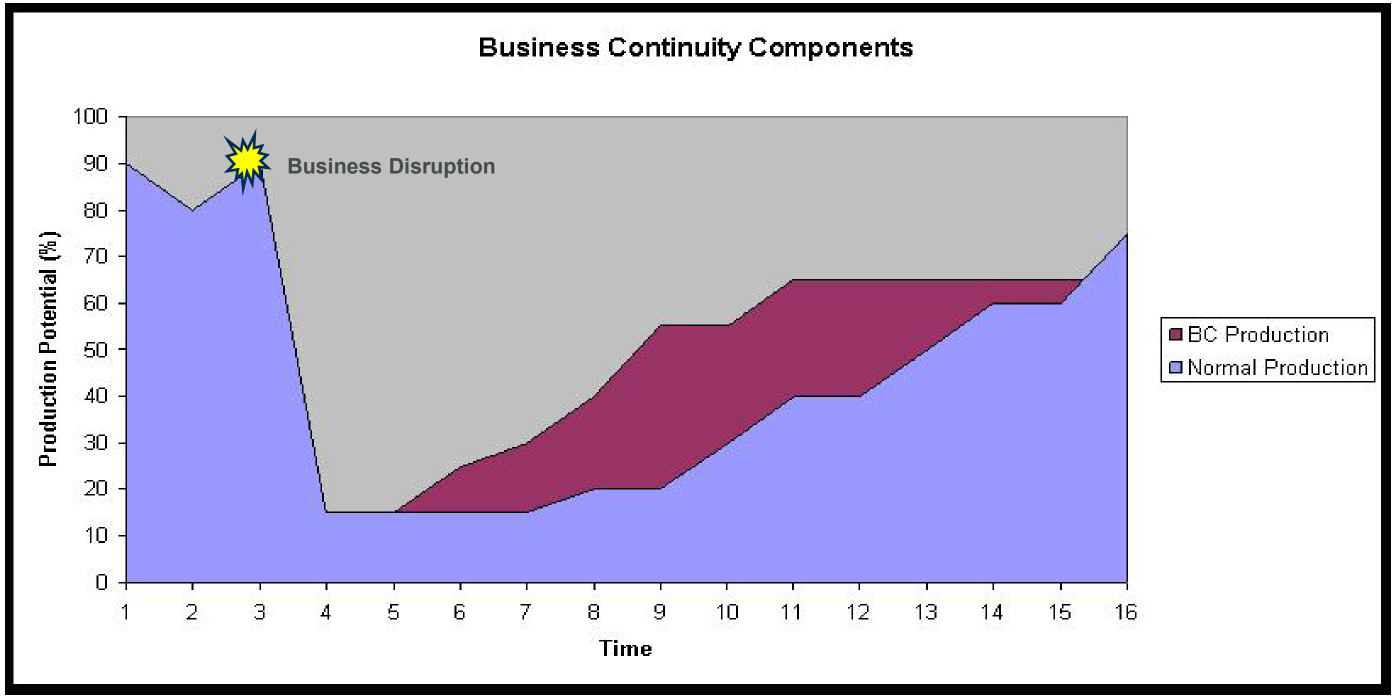
Principal, Managed Services Cybersecurity

Business Continuity

Business Continuity

Why Are Organizations Pursuing Business Continuity?

The focus of both business continuity and disaster recovery is to provide continuity of operations following an unexpected business disruption. Having plans in place allows an organization to minimize production losses until a full recovery can be made



What Is Business Continuity?

Business Continuity makes sure that critical operations can continue or recover quickly in the face of disruptions.

What Is Disaster Recovery?

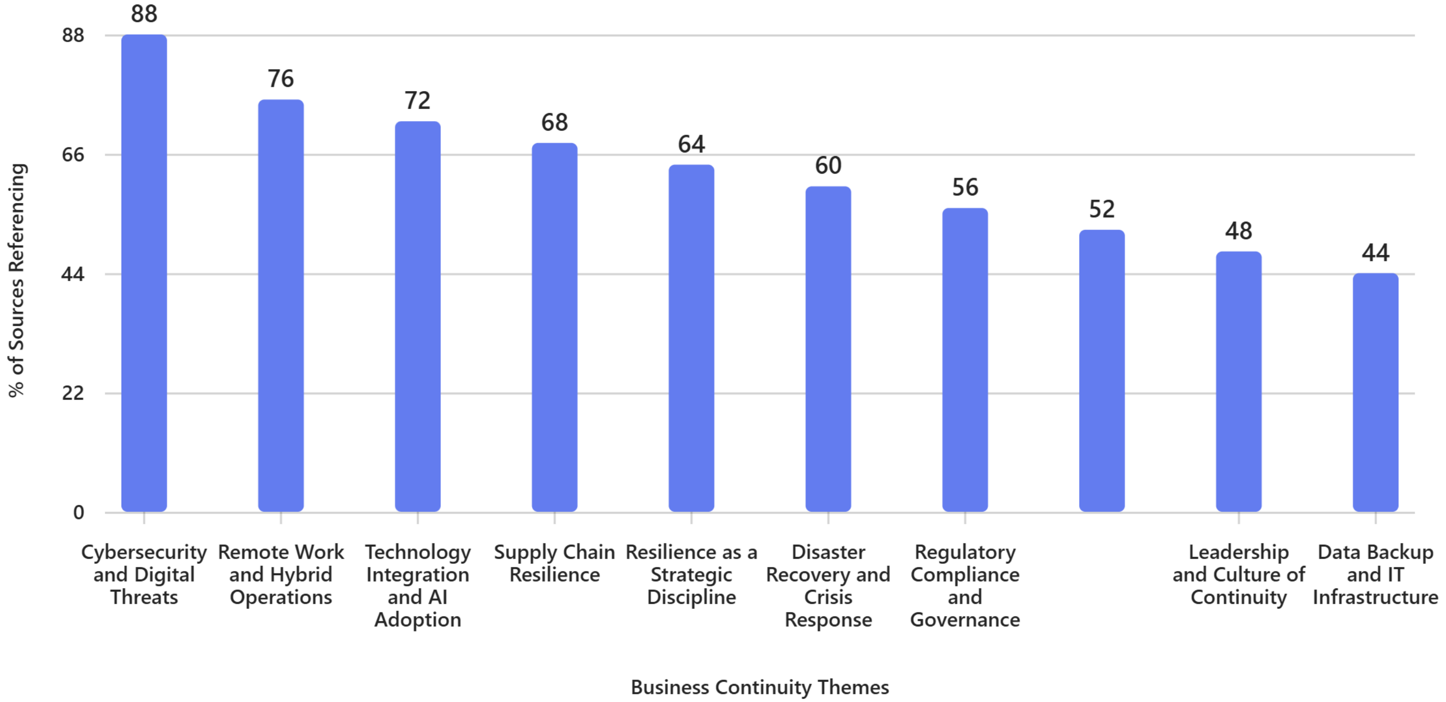
Disaster Recovery focuses on restoring critical IT systems, applications, and data after a disruption to safeguard rapid recovery and continuity of operations.

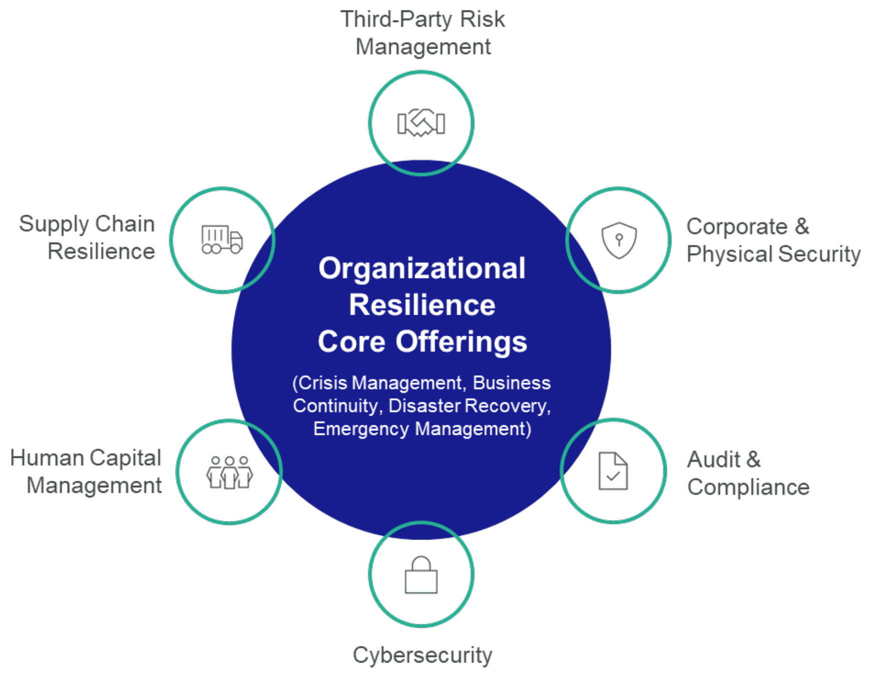
Business Continuity

What’s Trending in Business Continuity?

The overarching trend in business continuity from 2020 to 2025 is a strategic shift from reactive planning to proactive resilience—where organizations integrate technology, cybersecurity, and flexible operations to build adaptive systems capable of withstanding diverse disruptions

Review of over 100 publications focusing on business continuity and disaster recovery





Third-Party Risk Management
Supply Chain Resilience
Corporate & Physical Security
Organizational Resilience Core Offerings
(Crisis Management, Business Continuity, Disaster Recovery, Emergency Management)
Human Capital Management
Audit & Compliance
Cybersecurity

Common Audit Findings Related to Business Continuity

Key Takeaway: Organizations are expected to move beyond reactive planning and adopt a proactive, integrated approach to business continuity—one that embeds resilience across cybersecurity, operations, leadership, and compliance to ensure sustained performance amid disruption

BC/DR Theme	Common Audit Findings
Remote Work and Hybrid Operations	• Limited training and awareness for remote continuity roles • Inconsistent telework policies across departments
Supply Chain Resilience	• Failure to assess supplier continuity plans • Lack of visibility into Tier 2 and Tier 3 supplier risks • Inadequate vendor risk scoring and dur diligence • Poor documentation of supply chain disruptions and recovery strategies
Resilience as a Strategic Discipline	• Fragmented ownership of resilience across departments • Absence of a formal resilience framework or strategy • Limited executive oversight and board engagement • Reactive rather than proactive planning culture
Disaster Recovery and Crisis Response	• Misalignment between business continuity and disaster recovery plans • Lack of regular testing and simulation exercises • Incomplete documentation of recovery procedures • Overlooked dependencies between systems and functions
Regulatory Compliance and Governance	• Plans not aligned with ISO22301 standards • Missing documentation for compliance audits • Infrequent updates to continuity plans and governance policies • Lack of board-level reporting and oversight
Leadership and Culture of Continuity	• Low awareness of continuity roles among staff and leadership • Lack of training and engagement from senior management • Poor communication of continuity responsibility

Who's asking about business continuity?

FDA
U.S. Food and Drug Administration
Protecting and Promoting Your Health

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

OSHA®
Occupational Safety and Health Administration

CDC
CENTERS FOR DISEASE CONTROL AND PREVENTION

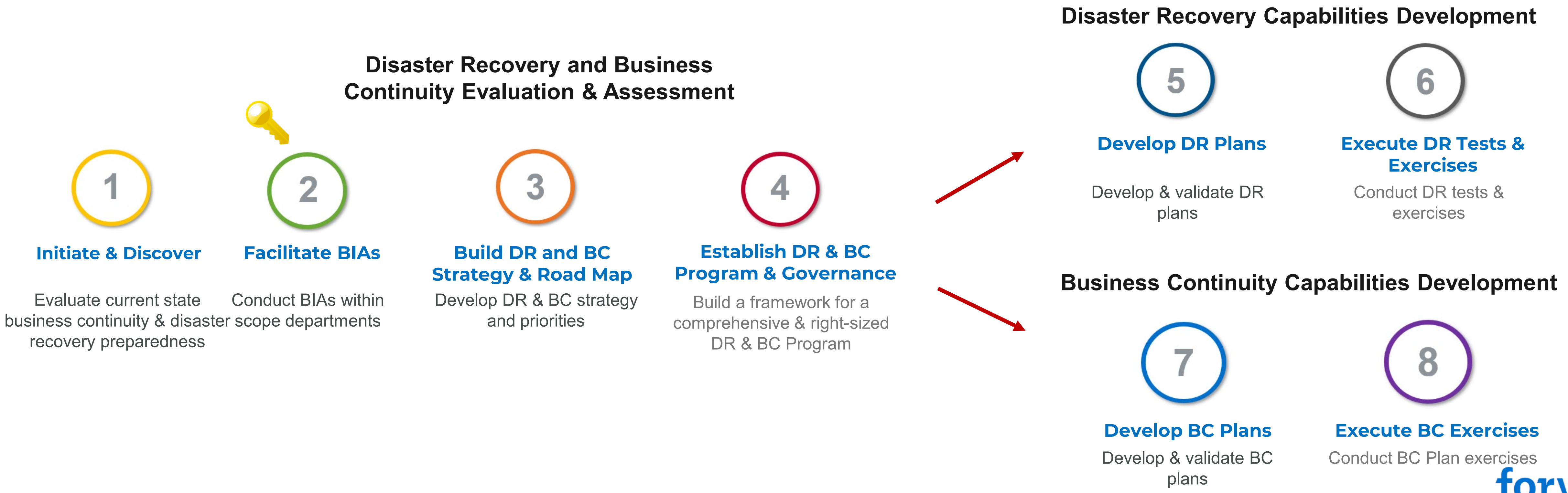
NIST

SOC 2

Real World BC/DR Project Plan

Successful Disaster Recovery (DR) and Business Continuity (BC) capabilities are not built in a vacuum. A successful and effective DR and BC Program requires the close collaboration of key decision makers and DR and BC subject matter experts to generate buy-in of the whole organization and build a culture of preparedness.

Increasingly, auditors, customers, and partners want to see a clear connection between critical business processes and supporting technologies and vendors/suppliers. The Business Impact Analysis is the core process that allows the business to define what business processes are most critical and to identify recovery strategies and targets for those processes to drive corresponding supply chain and disaster recovery activities.



Disaster Recovery and Business Continuity Evaluation & Assessment

1 **Initiate & Discover**
Evaluate current state business continuity & disaster recovery preparedness

2 **Facilitate BIAs**
Conduct BIAs within scope departments

3 **Build DR and BC Strategy & Road Map**
Develop DR & BC strategy and priorities

4 **Establish DR & BC Program & Governance**
Build a framework for a comprehensive & right-sized DR & BC Program

Disaster Recovery Capabilities Development

5 **Develop DR Plans**
Develop & validate DR plans

6 **Execute DR Tests & Exercises**
Conduct DR tests & exercises

Business Continuity Capabilities Development

7 **Develop BC Plans**
Develop & validate BC plans

8 **Execute BC Exercises**
Conduct BC Plan exercises

forvis mazars

Cyber & Organizational Resilience

Cyber & Organizational Resilience

The Key Challenge

Ability to Anticipate, Withstand, Recover From, & Adapt to Cyberattacks

Problems/Threats

- Threat Volume
- Complexity
- Speed Outpaces Human Capability
  - Resource Shortage
  - Skill Gaps
  - Alert Fatigue
  - Alert Dwell Times

Observations

- Rapid Threat Evolution Is Outpacing Security Capabilities
- 90% of Organizations Lack the Maturity to Defend Against AI-Enabled Threats
  - *i.e.*, Sophistication & Volume of Threats:
    - Polymorphic Malware
    - AI-Driven Phishing
    - Deepfake Scams

Opportunity

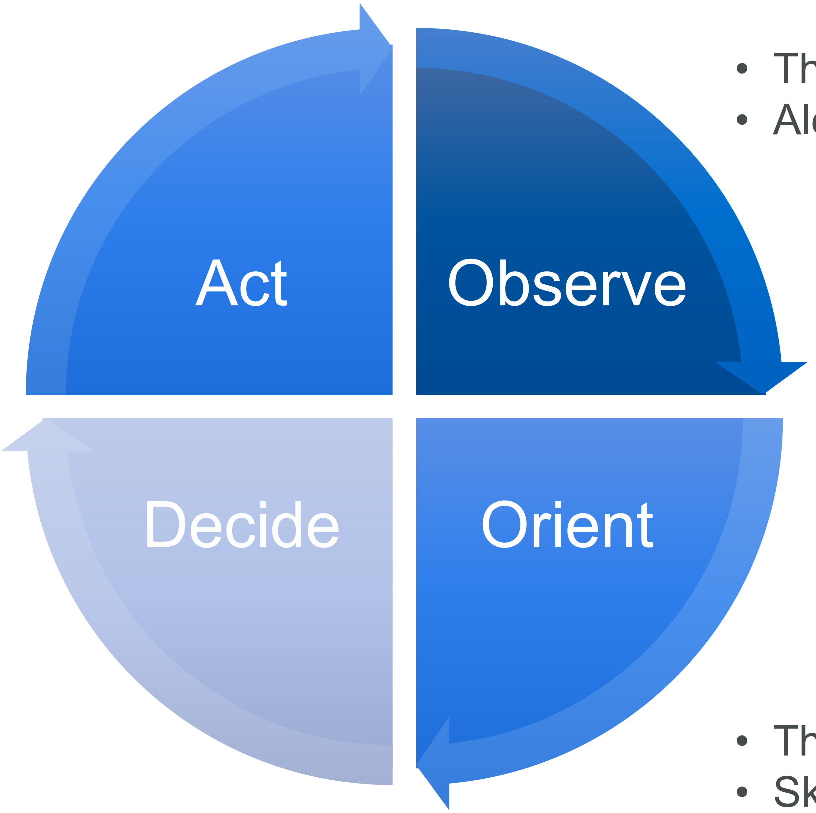
- AI Is Here—for Better & Worse
- The Technology & the Market Say We Must Adapt & Evolve
- **How Do We Effectively & Responsibly Consider & Implement AI for Cyber Operations Resilience?**

Cyber & Organizational Resilience

Traditional OODA Loop

- Cyber operations process – OODA loop
- Current challenges & resiliency risk points
- Identify where AI can augment (not replace)
- AI augmentation paired with a human in the loop (HITL) strategy for operations improvement

Current Problems/Threats



- Threat Volume
- Alert Fatigue

- Threat Complexity
- Skill Gaps

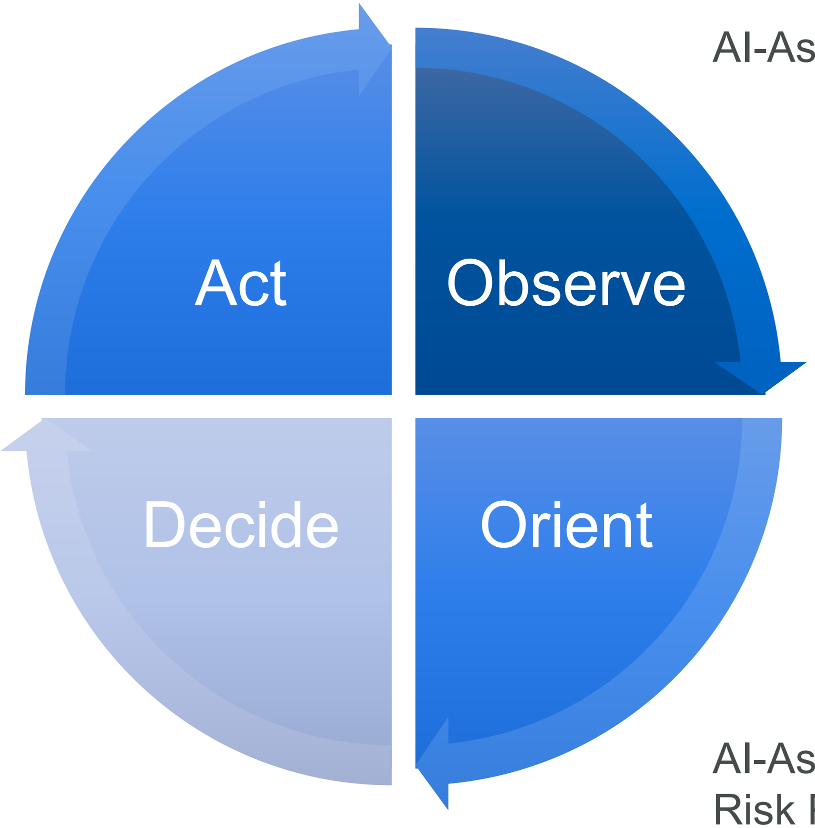
- Threat Speed
- Skill Gaps

- Skill Gaps
- Dwell Time

Cyber & Organizational Resilience

How Do We Evolve OODA Loop?

- Identify where AI can augment (not replace) & enhance operations
- Maintain HITL for necessary oversight & execution of service delivery


Current Problems/Threats
AI-Assisted Data Collection
Act
Observe
AI-Assisted Correlation & Analysis
AI-Assisted Remediation Recommendations
Decide
Orient
AI-Assisted Investigation, Risk Prioritization

Cyber & Organizational Resilience

AI-Augmentation, Not Replacement

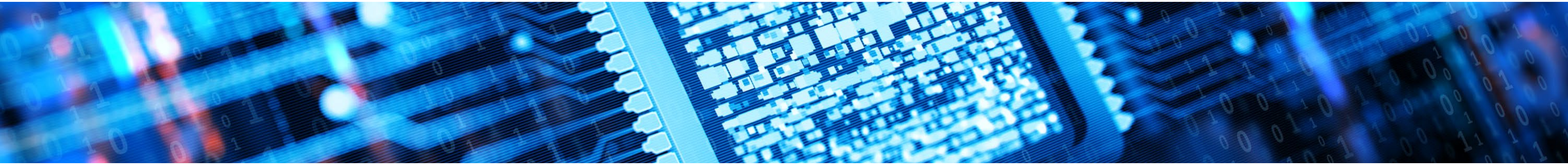
Why Not Total Replacement

Even with rapid evolution of AI, agentic AI & its benefits, we're not ready for completely autonomous cyber operations

AI lacks human business context, unique situational knowledge

AI may struggle with threat patterns that it is not trained on

AI may have algorithmic bias or errors in its results



Cyber & Organizational Resilience
AI-Augmentation, Use Case #1

AI-Assisted SOC Analyst

- OODA Challenge:
  - Observe – threat alert volume
  - Orient – how to correlate threat activity across data source types
  - Decide – investigation questioning & conclusions
  - Act – thorough remediation

- Goals/Use Case:
  - Reduce SOC activity with false positives
  - Improve SOC metrics (mean time to detect, investigate, respond, close)
  - Improve SOC analyst quality
  - Improve SOC analyst alert fatigue

- AI-Assisted Process:
  - Security event alerts are received (SIEM)
  - AI-augmentation for investigation & analysis
    - Autonomous investigation
      - Breadth & depth of queries, responses, follow-up queries, correlations, & analysis
      - Investigation outcomes pushed to SIEM/SOAR for case management
  - SOAR integration
    - Auto-closure of benign cases
    - Confirmed threat activity:
      - Investigation details attached as case artifacts for SOC analyst validation
      - SOC playbook execution (escalation, closure, etc.)
- Goals/Benefits:
  - Reduce false positives (~80% of all SOC work)
  - Augment team for enhanced investigation capabilities (speed, accuracy)
    - Seen evidence of 15–50 questions being asked during a case investigation that on average is determined within **3–10 minutes**, which is a significant time savings

Cyber & Organizational Resilience
AI-Augmentation, Use Case #2

AI-Assisted Vulnerability Management

- OODA Challenge:
  - Observe – vulnerability scan reports are extremely long
  - Orient – difficult to interpret
  - Decide – hundreds, thousands of report pages are almost unactionable
  - Act – reports are often dismissed or deprioritized

- Goals/Use Case:
  - Challenging & unactionable vulnerability scan reports
  - Reduce organizational risk with enhanced & efficient vulnerability identification, processing, & remediation

- AI-Assisted Process:
  - Deploy agentic AI vuln. management solution
  - Integrate vuln. mgmt. inputs into AI reasoning engine:
    - Data sources (scan reports, systems infra, cloud web app, threat intel, etc.)
    - Organizational context (business, network playbooks, policies)
    - Define outcomes (risk reduction, compliance, etc., as prompt tasks)
  - Reasoning Engine:
    - Integrates & processes vuln. database, inference, prompt templates, context engineering, unified data model, deep reasoning, LLM orchestration
    - Attack path discovery & actionable output report
- Benefits/Outcome:
  - Actionable risk prioritization
  - Autonomous vuln. mgmt. analyst
  - Streamlines tasks to reduce friction & create alignment between vuln. management & infrastructure teams
  - Offloads high-effort, low-value tasks to AI agent, making vuln. scan reporting actionable

Cyber & Organizational Resilience

AI-Augmentation, ROI

Conclusion

Seek to Understand How & Where AI Can be Leveraged to Enhance Organizational Resilience

Identify Risk

- Identify where there is risk within the current cybersecurity operations workflow
- Operational:
  - Is this within the SOC monitoring, investigation, response capability?
  - Is this within the vulnerability management process?
  - Other?
- Strategic:
  - Is this within governance around IT or security? Policy updates, maintenance, enforcement, or mapping to compliance requirements?

Based on Risk Results, Identify & Prioritize Use Cases

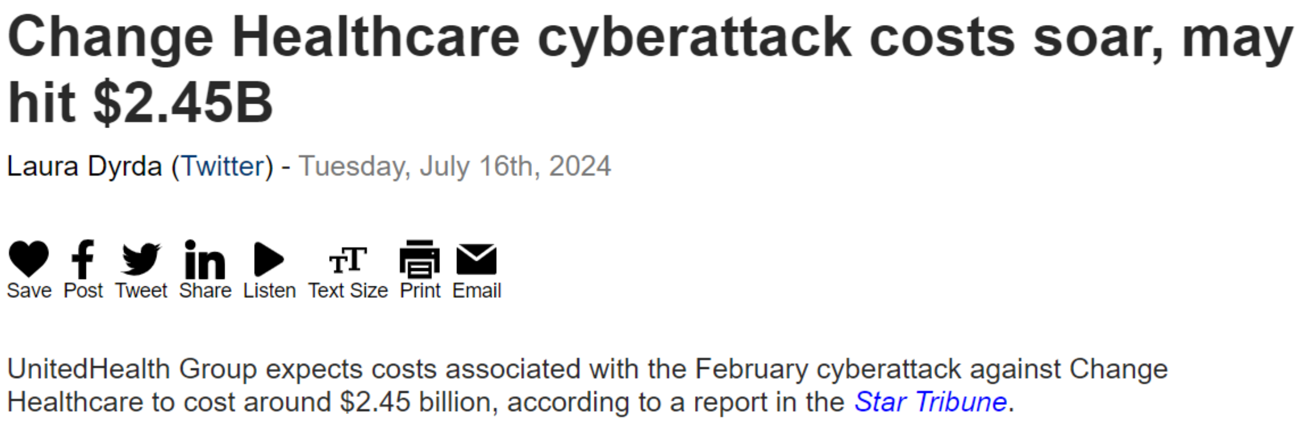
Implement

Cybersecurity

Cybersecurity

Recent Cyber Events

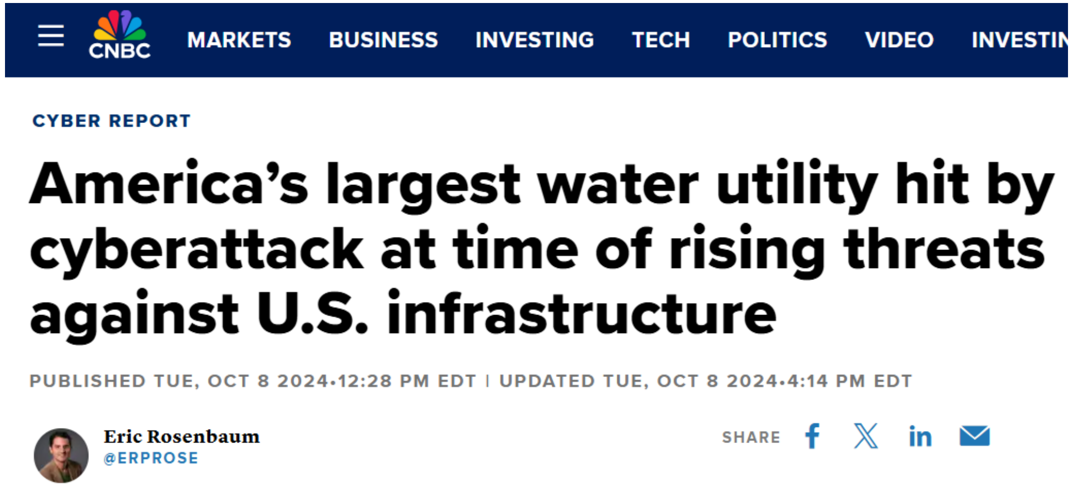
Headlines



Change Healthcare cyberattack costs soar, may hit $2.45B

Laura Dyrda (Twitter) - Tuesday, July 16th, 2024

UnitedHealth Group expects costs associated with the February cyberattack against Change Healthcare to cost around $2.45 billion, according to a report in the *Star Tribune*.

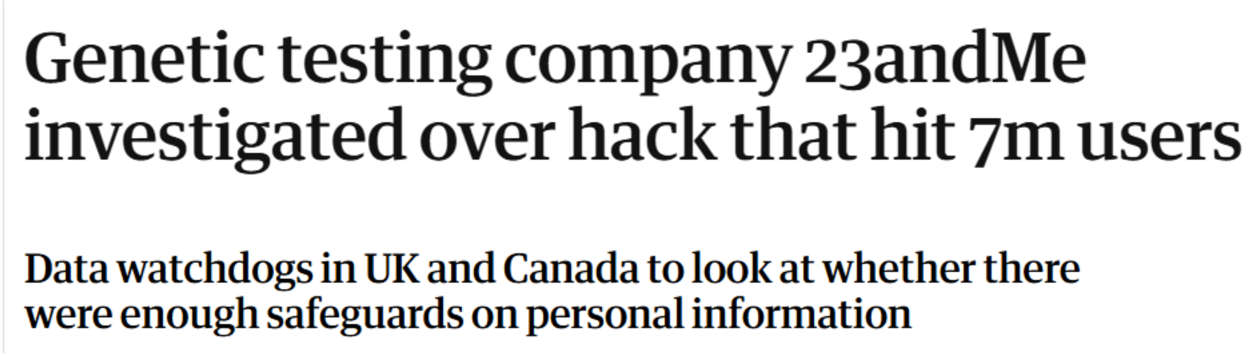


CYBER REPORT

America's largest water utility hit by cyberattack at time of rising threats against U.S. infrastructure

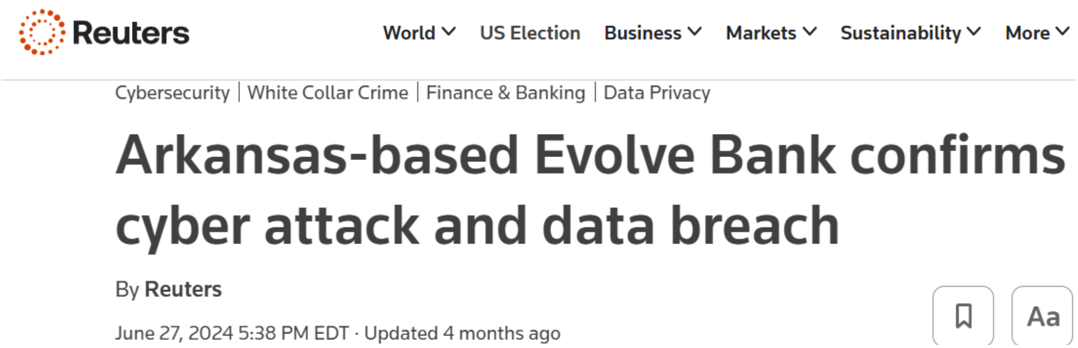
PUBLISHED TUE, OCT 8 2024·12:28 PM EDT | UPDATED TUE, OCT 8 2024·4:14 PM EDT

Eric Rosenbaum
@ERPROSE



Genetic testing company 23andMe investigated over hack that hit 7m users

Data watchdogs in UK and Canada to look at whether there were enough safeguards on personal information



Cybersecurity | White Collar Crime | Finance & Banking | Data Privacy

Arkansas-based Evolve Bank confirms cyber attack and data breach

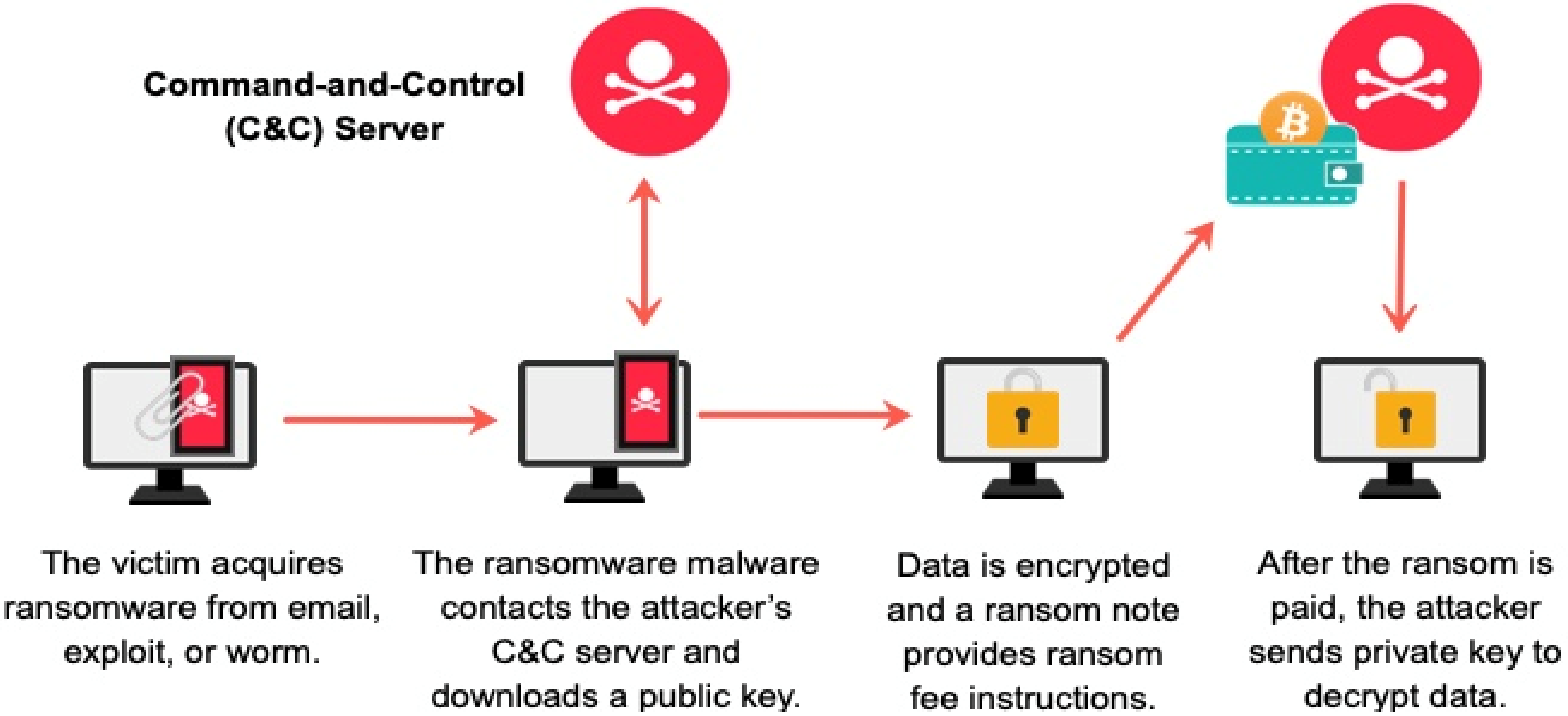
By Reuters

June 27, 2024 5:38 PM EDT · Updated 4 months ago

Cybersecurity

What Is Ransomware?

Ransomware is a type of malware that locks files on a victim machine, making data inaccessible. A ransom note appears on the victim’s computer with instructions for paying the attacker (usually in a cryptocurrency such as Bitcoin) to unlock the files. Typical attacks are originated from email attachments, malicious links, or malware.



The victim acquires ransomware from email, exploit, or worm.

The ransomware malware contacts the attacker’s C&C server and downloads a public key.

Data is encrypted and a ransom note provides ransom fee instructions.

After the ransom is paid, the attacker sends private key to decrypt data.

Source: ExtraHop

Cybersecurity

Changes to Cybercrime Landscape

Ransomware Gangs

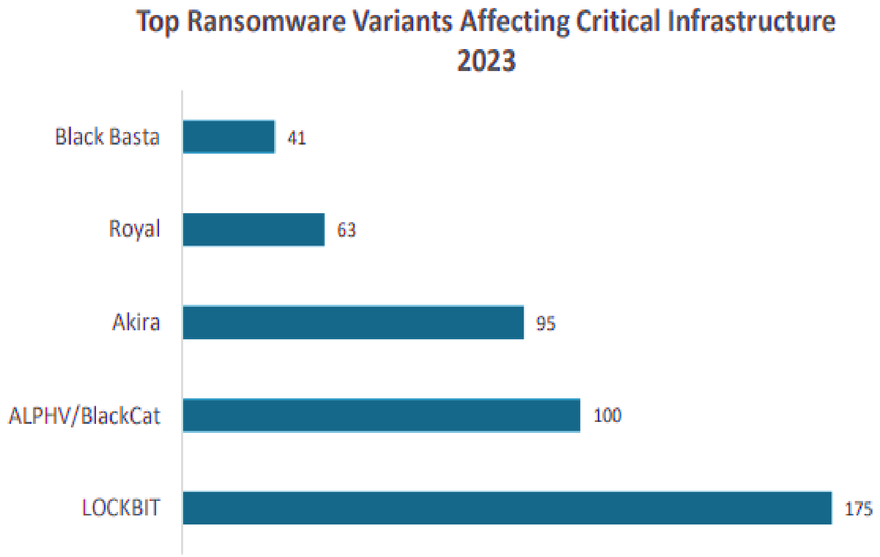
$1.1 Billion Ransom payments collected in 2023 [4]

The **United States** is the most targeted country targeted by **LOCKBIT3.0.**

Conti **expressed support for the Russian government** and threatened to target "enemies."

ALPHV/BlackCat is a veteran group that was responsible for the **Colonial Pipeline.**

Top Ransomware Variants Victimizing Critical Infrastructure – 2023 Incidents [1]



Ransomware Innovation

Internal files showed ransomware groups are exploring advanced new techniques. [2]

Buying the same EDR tools we use to test their weaknesses

Using blockchain smart contracts to expedite ransom payment

Creating their own decentralized finance platforms

"Big companies have too many secrets that they hold on to, thinking that this is their main value, these patents and data."

Ransomware Leader

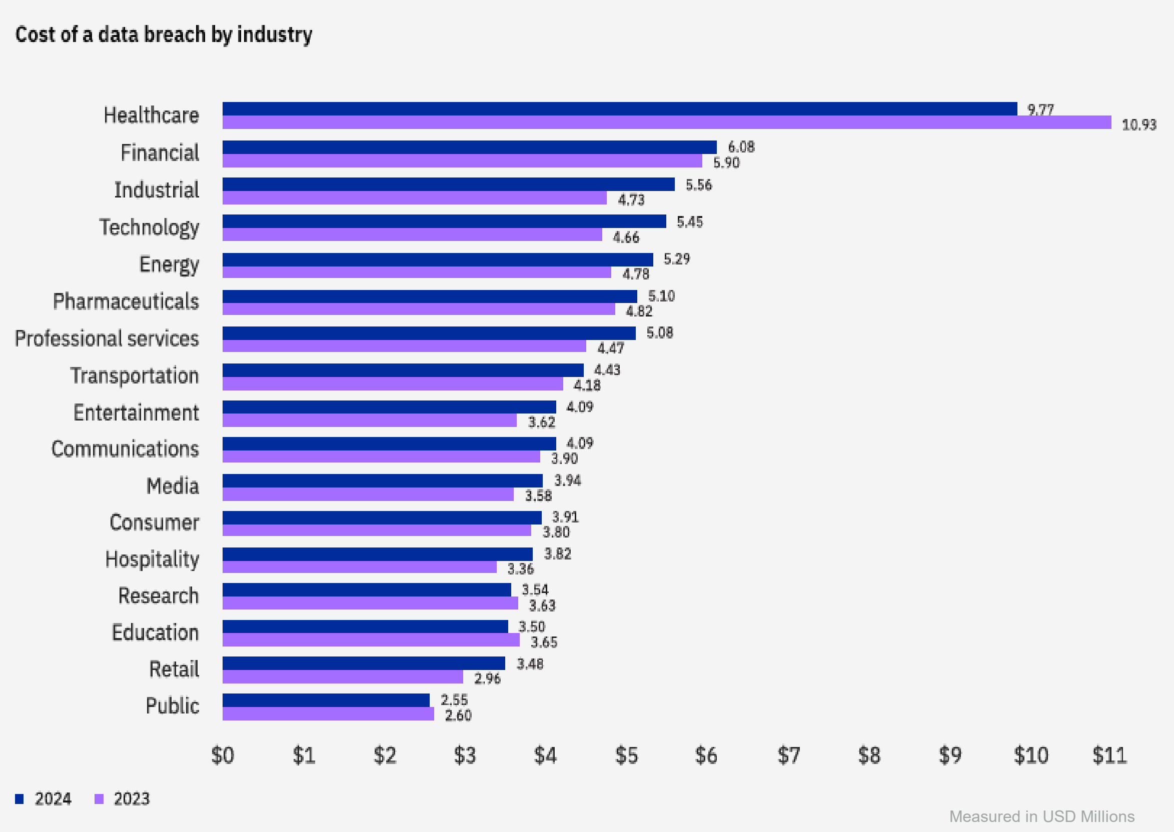
Threat actors are using AI to develop phishing emails, automate attacks, spread ransomware, rapidly exploit vulnerabilities, and develop complex malware code.

[1] 2023 FBI Internet Crime Report
[2] Conti Ransomware Group Diaries, Part IV: Cryptocrime – Krebs on Security. Krebsonsecurity.com.
[3] Political fallout in cybercrime circles upping the threat to Western targets – Cyber Scoop. cyberscoop.com.
[4] Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline - Chainalysis

Cybersecurity
Statistics & Financial Impacts

Cost of a Data Breach & Ransomware

Ransomware attacks are easier and more inexpensive to pull off, while offering the prospect of very high rates of return for cybercriminals.



Source: 2024 IBM Cost of a Data Breach Report

USD $9.36 Million

Average cost of a breach in the United States, the highest of any country

258 days

Average time to identify and contain a data breach

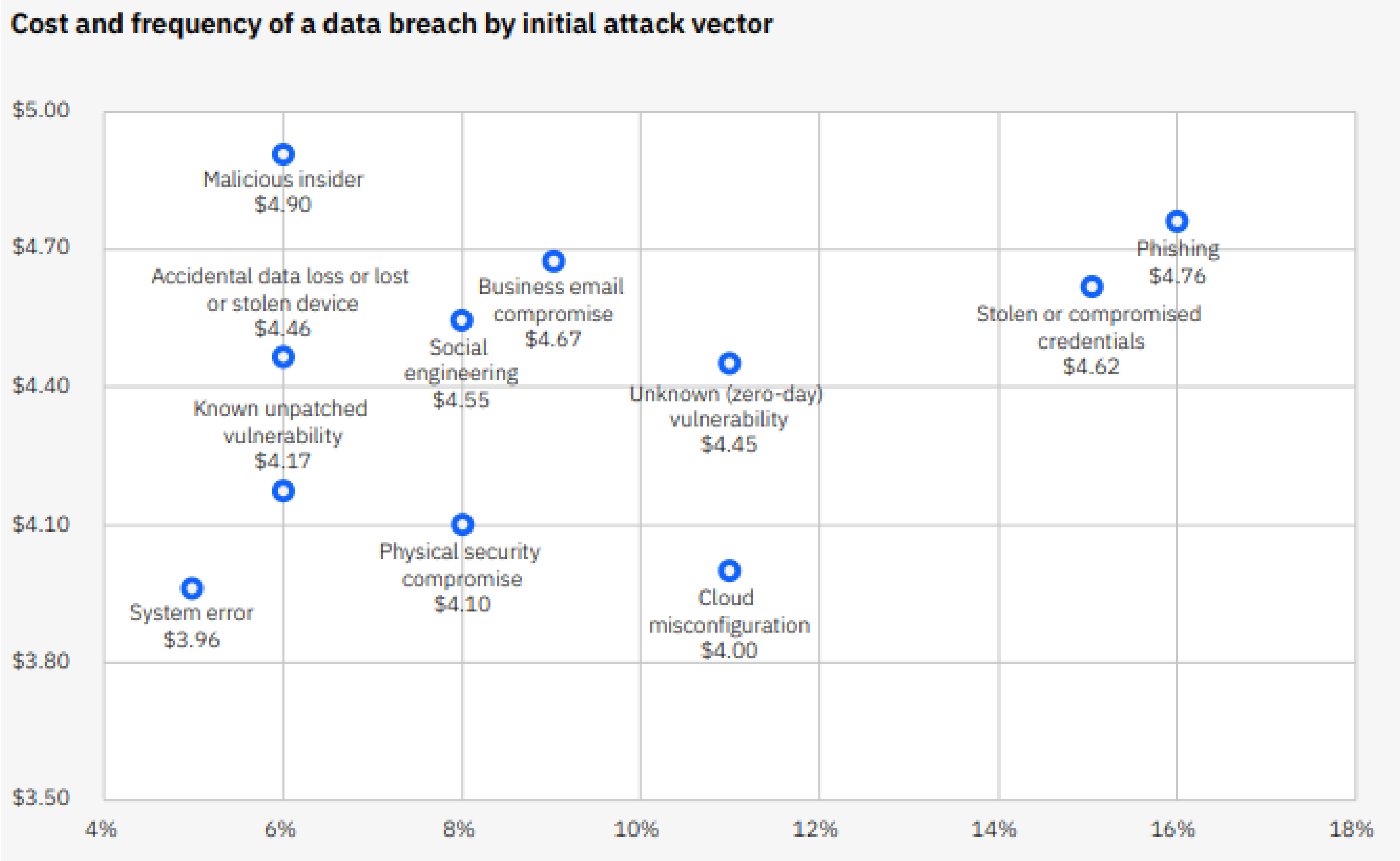
2.2 Million

Average savings of a breach when AI Security and Automation was utilized

Data breaches in high data protection regulatory environments and **critical infrastructure** tended to see costs accrue in later years following the breach. In ***highly regulated industries***, an average of **24% of data breach costs was accrued more than two years** after the breach occurred. Regulatory and legal costs may have contributed to higher costs in the years following a breach.

Cybersecurity

Statistics & Financial Impacts: Attack Vectors by the Numbers



Phishing and stolen or compromised credentials were responsible for 16% and 15% of breaches.

In 2023 cloud misconfiguration was identified as the initial vector for 11% of attacks, followed by business email compromise at 9%

Attacks initiated by malicious insiders were the **costliest**, at an average of USD $4.90 million, which is 9.6% higher than the global average cost of USD $4.45 million per data breach..

Cybersecurity **Recommendations**

Don’t be the next news headline. Once an incident occurs, it is too late!

Implement a proactive approach.

Perform a Risk Analysis

Can be framework-specific, entitywide, or both. A Risk Analysis should evaluate inherent and residual risks to the organization. A risk score should be associated with each functional area of the Risk Analysis.

Perform a Controls-Based Assessment

Utilize a well-recognized controls framework to assess the organization’s security posture. Develop corrective action plans to formalize, assign, and track identified vulnerabilities to completion. Incorporate a cyber technical assessment.

Cybersecurity
Incident Response Table-Top Exercise

What is a table-top exercise?

A coordinated effort to discuss hypothetical emergency scenarios and how key stakeholders of an organization might react. The exercise should be guided by the organization’s incident response plan and capture lessons learned from the discussions.

Goals & Objectives

1. Better understand roles
2. Create a safe space for critical thinking
3. Instill confidence
4. Education and training
5. Process improvement

Cybersecurity
Case Study

Incident Response Procedures

Recent security incidents led to a client reaching out with concerns regarding their incident response procedures. After discovery sessions, Forvis Mazars developed a plan to perform a three-scenario table-top exercise to help evaluate incident response at the entity level.

Client

- Medical & Tubing Manufacturer
- Organization spans two facilities with one main operations center
- Approximately 200 employees

Scenarios

Ransomware

Environmental Disaster

Vendor Security Incident

Forvis Mazars served as the developers and facilitators of the three disaster narratives and table-top exercise sessions.

Cybersecurity
Case Study Analysis

Communication was a big issue

Decision-making processes were unclear

Collaboration is hard but key to success

Defining roles was critical

Hesitation to declare a disaster was prominent

Education and training were desperately needed

Q&A

Cyber & Organizational Resilience

Questions?

Contact

Forvis Mazars

Justin Hill
Lead Consultant, CFO & Business Consulting
P: 906.268.9316
justin.hill@us.forvismazars.com

Ben Doane
Principal, Managed Services Cybersecurity
P: 646.306.0913
ben.doane@us.forvismazars.com

Ben Owings
Director, IT Risk & Compliance
P: 704.644.4859
ben.owings@us.forvismazars.com

The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and 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 and 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 and legal authorities.