Cybersecurity Threat Landscape

Mark Ward (SVP, Chief Information Security Officer)

May 1, 2025

JOHNSON FINANCIAL GROUP®

Cost of a Data Breach

Breach related financial impacts…

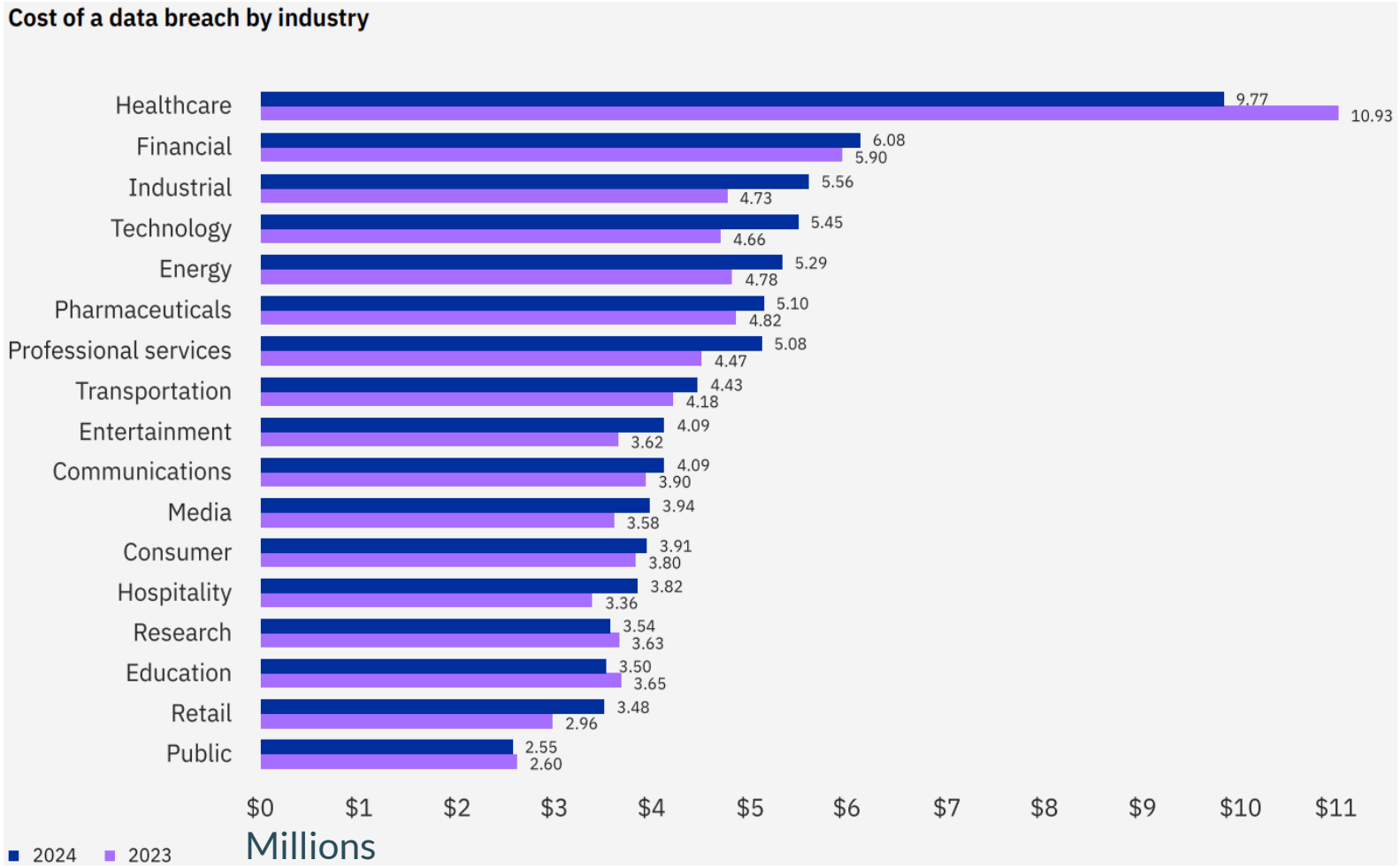
Lost Business (~39%): Lost revenue, customer churn, downtime, reputational damage, and SLA penalties

Detection & Escalation (~28%): Time and effort to detect, triage, investigate, and forensics to confirm the breach.

Post-Breach Response (~27%): Legal fees, regulatory fines, PR/Crises communication, customer notification, credit monitoring

Notification (~6%): Creation and delivery of breach notifications to regulators, customers, and partners.

Cost **increased 9.7%** from $4.45M in 2023 to **$4.88M in 2024**



Source: IBM, "Cost of Data Breach Report 2024"

Cyber Attack volume, quality, and speed are increasing!

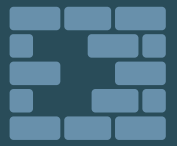
Cybersecurity defenders need to be right 100% of the time, the **attackers only need to be right once!**

Cyber threat detection and response is no longer a human scale problem!

- Throughout 2024 into 2025, 50,000+ reported cybersecurity incidents with almost 23,000 confirmed data breaches.
- The time the attacker requires to move from the initial point of compromise to other assets on company networks, aka 'breakout time', is now down to an average of 48 minutes with the fastest reported at 51 seconds!
- Every month even SMB's have billions of logged events, correlating to thousands of incidents to be analyzed, with tens or hundreds of true-positive incidents to contain and respond to 24x7x365!
- Ransomware as a Service (RaaS) has lowered the bar to less sophisticated attackers getting in the game increasing the overall volume of ransomware attacks.
- Ransomware is present in 44% of global breaches, 70% of small business breaches and over 90% of mid-sized business breaches.

Small business (less than 500 employees), Medium business (500-5,000 employees)

Vulns & Weak Configurations



Over 30% of all breaches were the result of attackers exploiting vulnerabilities and poorly configured (weak) systems because of ‘human error’.

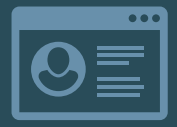
- There were 40,000+ vulnerabilities published in 2024.
- 13.7% (5,481) classified as ‘Critical’.
- A substantial number of these critical vulns allowed unauthenticated remote code execution (RCE).
- AI tools help attackers quickly and accurately build exploit code for newly announced vulnerabilities.
- Infostealer malware surged in 2024 exploiting system vulnerabilities stealing over 2.1 billion credentials accounting for more than 60% of all credentials stolen last year.

Email Security

Over 90% of global email traffic is categorized as spam, encompassing unsolicited, unwanted, or malicious content.

- Most attacks still start with socially engineering people with phishing, smishing (fake SMS texts), and vishing (fake voice calls).
- 442% increase in AI assisted vishing (fake phone call) attacks in the last year which are often correlated to support the success of phishing and smishing attacks.
- BEC (Business Email Compromise) increased nearly 250% year over year, now makes up approximately 8.5% of all data breaches, are more targeted than typical phishing often asking for sensitive information or transferring funds by impersonating trusted individuals or organizations and cost companies an average of $4.67 million per attack.

Credential Abuse & Theft



Most annual cybersecurity reports have credential theft and abuse as a leading or top 3 attack vector.

- The initial access of many attacks are malware-free often involving stolen credentials.
- Increased risks from accessing company systems from unmanaged assets, impacting digital identity security.
- Smishing (fake SMS texts) attacks have increased significantly, bypass traditional email security and deceive victims into revealing credentials.
- Weak or reused compromised passwords are a major factor in credential abuse and theft.

3rd Party Supply Chain

30% of breaches involved third parties, doubling from the previous year.

- Exploitation of vulnerabilities within third-party supply chains now accounts for about 30% of breaches making it a high cybersecurity risk.
- Unmanaged data sources in third-party environments are increasing the complexity and cost of breaches.
- Vulnerabilities in third-party software and cloud services increasingly being used for initial access, data theft, and lateral movement into customer networks.

Don’t be the easy to get, ‘Low Hanging Fruit’!

1. **Patch and update systems** within 30-day cycles to reduce your attack surface. Some critical vulnerabilities allow Remote Code Execution (RCE) without authentication!
2. **Enforce Multi-Factor-Authentication (MFA) everywhere** (especially with privileged accounts!). Someone in your company will eventually fall for a social engineering attack. Don’t let weak and reused compromised passwords to be your downfall.
3. **Start from hardened secure configurations** like CIS Benchmarks for your internally managed and cloud-based builds. Don’t let limited in-house cybersecurity capabilities and human error open your company to attacks.
4. **Maintain regular backups,** daily and ‘immutable’, and test recovery regularly. You will eventually need them!
5. **Deploy** the best **Email Security**, **EDR** (Endpoint Detection & Response), and **Managed Security Operations Services** you can afford! Detecting, analyzing, containing, and responding to cyber threats requires qualified people watching 24x7x365 using automation and AI assisted analysis to keep up with AI assisted and automated attacks. Don’t be an easy low-cost target, and the next headline.
6. **Monitor your third-party supply chain**, and yourself, with scoring services (BlackKite, SecurityScorecard, BitSight, others) to quickly find and remediate the weakest link in your chain.

Other Helpful Resources to Consider…

- Control Frameworks
  - ***CIS Critical Controls:*** *Prioritized controls with clear language mapped to other compliance frameworks, built on best practice cyber threat models like MITRE ATT&CK offering many free resources. (https://www.cisecurity.org/controls)*
  - ***NIST Small Business Cybersecurity Corner:*** *Cybersecurity basics for small businesses with free resources. (https://www.nist.gov/itl/smallbusinesscyber)*
- Free Daily Cyber Threat Intelligence Podcasts (~15min; ~7min each)
  - ***Cyber Security Headlines*** *(https://cisoseries.com/category/podcast/cyber-security-headlines/)*
  - ***SANS Internet Storm Center*** *(https://isc.sans.edu/podcast.html)*

- Free Security Scores:
  - *Even if you don't have budget for a cybersecurity scoring services like BlackKite, SecurityScorecard, or BitSight to monitor you and your critical third-party supply chain vendors, check out their sites for a* ***FREE report on your company's domain****.*

Sources

If you would like to do a deeper dive into the data…

- **Verizon** 2025 Data Breach Investigation Report (18th edition)
- **Crowdstrike** 2025 Global Threat Report (9th edition)
- **ReliaQuest** 2025 Annual Cyber-Threat Report (7th edition)
- **Mandiant** M-Trends 2025 (16th edition)
- **IBM/Ponemon** Cost of a Data Breach Report 2024 (19th edition)
- **Sophos** Annual Threat Report "Cybercrime on Main Street 2025 (12th edition)

Thank You

Mark Ward
SVP, Chief Information Security Officer
Johnson Financial Group

JohnsonFinancialGroup.com

JOHNSON FINANCIAL GROUP®

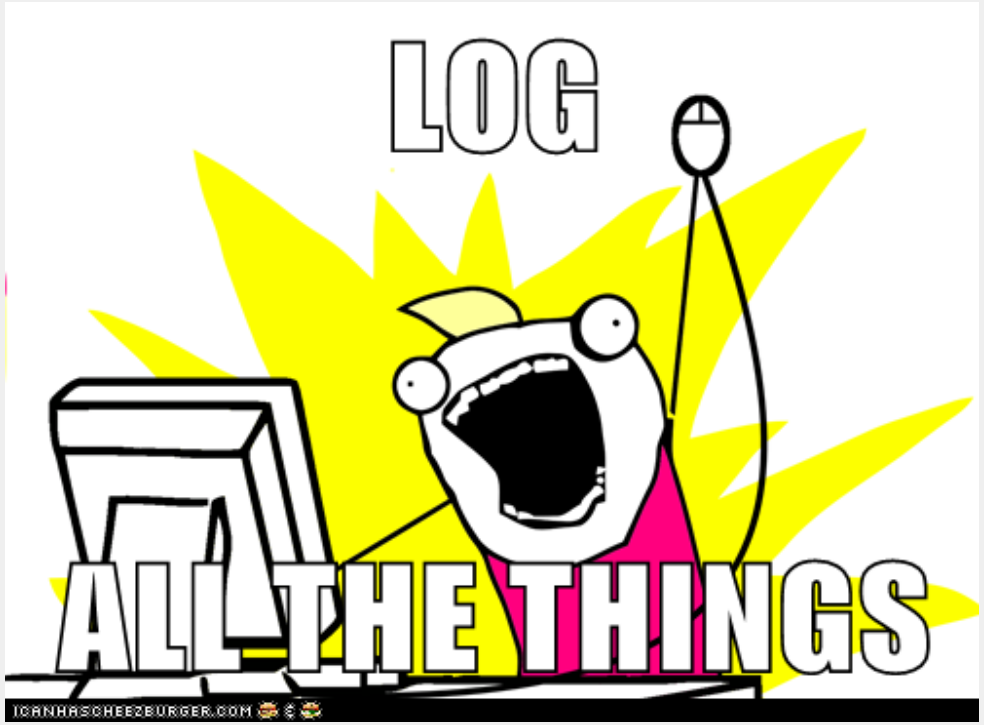
Responding to a Ransomware Event

Immediate IT Response

- Isolate affected systems by restricting external network traffic to prevent further damage:
  - Removing network cables
  - Network contain systems in EDR
  - Disable virtual network connections
- Secure and validate backups
- Reset admin passwords
- Check firewall for active suspicious connections
- Pause scheduled maintenance tasks that overwrite logs or overwrite backups
- Do not start wiping systems!

Evidence to collect

- Ransom note and sample encrypted files
- EDR and live response data
- Firewall and VPN logs
- Endpoint triage data
- Forensic images/virtual disks
- Cloud logs/email logs
- Application logs
- Employee interview
- Web filter logs
- Netflow logs



Evidence Preservation

Image/collect artifacts from key servers

- Domain Controllers
- Terminal Servers
- File Servers (operating system drives)
- Servers that contain sensitive info

Note:

- For virtual servers collect the VMDK or VHD files along with the associated files contained in the VM folder.
- Systems that do not show signs of encryption are often used as staging points; do not assume they were not accessed.

Investigate

- Patient 0 / Entry Point
- Privilege Escalation
- Persistence
- Lateral Movement
- Data Access/Exfiltration
- Encryption
- Goal (Extortion for Ransom)

Why Communicate With Threat Actor?

Prevent/Delay Harassment

Prevent/Delay Posting

Obtain List of Exfiltrated Files

Confirm Data Exfil

Proof of Life

Communication Methodology

- .txt file dropped on system
- File extension
- Extortion emails
- Web form submission
- Blog announcement

- Chat panel
- Email
- qTox
- Telegram/Signal
- Session

- Exfiltrated data list?
- Encryption impact
- Demands
- Get proof of data theft

- Determine end goal
- Delay tactics include holidays, weekends, proof exercises, leadership meetings.
- Or purchase decryptor

CRA Charles River Associates

Communication Methodology

- .txt file dropped on system
- File extension
- Extortion emails
- Web form submission
- Blog announcement

- Chat panel
- Email
- qTox
- Telegram/Signal
- Session

- Exfiltrated data list?
- Encryption impact
- Demands
- Get proof of data theft

- Determine end goal
- Delay tactics include holidays, weekends, proof exercises, leadership meetings.
- Or purchase decryptor

CRA Charles River Associates

Thank You

Ryan Irish | Panelist | TG3 Electronics Inc
Adam Hart | Panelist | Charles River Associates
Dave Cunningham | Panelist | Alvaka Networks

JohnsonFinancialGroup.com

JOHNSON FINANCIAL GROUP®