HALOCK®

- Security Briefing

September 25th, 2025

About the Presenter

- Founding Partner of **HALOCK Security Labs** (1996)
- *Board Member of the **DoCRA Council***

  ("Duty of Care Risk Analysis")
- Contributing author of the CIS RAM

  Center for Internet Security Risk Assessment Method
- Litigation support for large cyber breaches
- Over 35 years of experience in IT and Security
- Strategic Partnerships for Reasonable Risk SaaS
- ISO 27001 Auditor, CISA, CISSP
- University of Wisconsin with a B.S. in Computer Science ('92)

Terry Kurzynski,

Board Member, The DoCRA Council

Founder, HALOCK Security Labs

Partner, Reasonable Risk SaaS

Cars, Guitars and Cocktails

HALOCK®

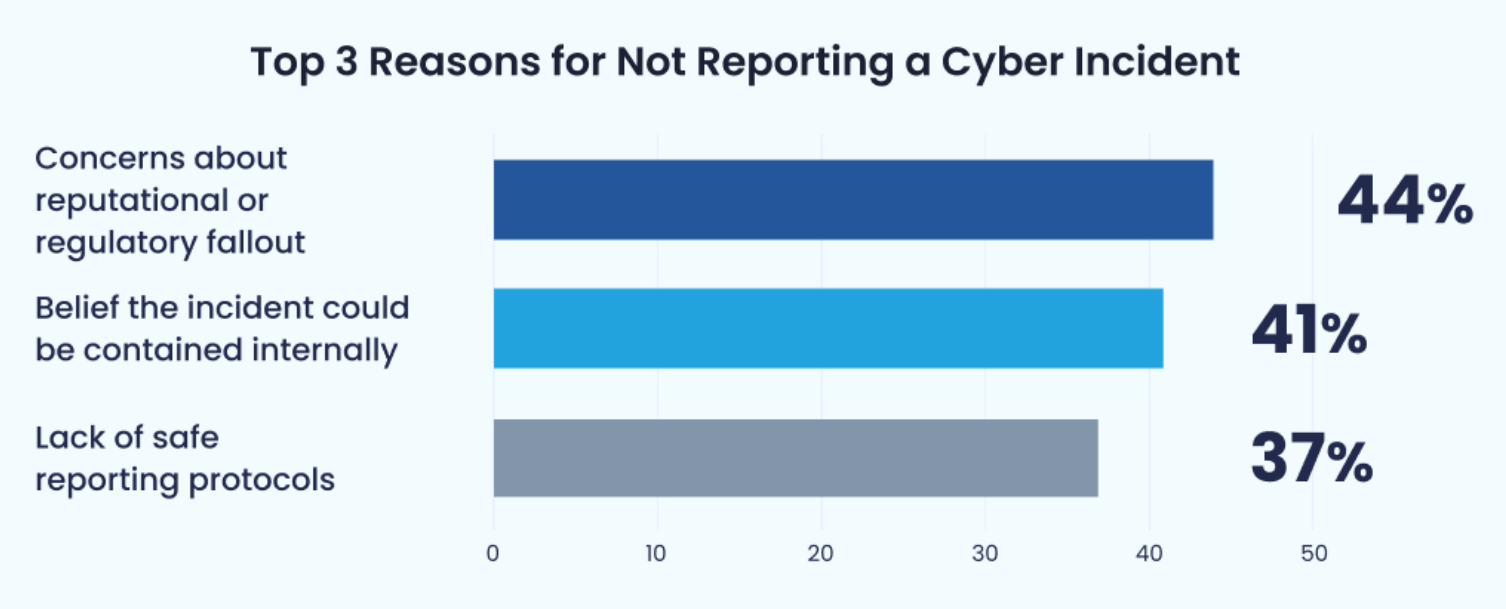
Cyber Stats and Facts 2025

09/16/2025

- Cybercrime is set to cost businesses up to $10.5 trillion in 2025.
- Business owners view cyber risks as more threatening than any other cause of business loss – at 34% – surpassing natural disasters.
- 97% of companies report GenAI security issues.
- Up to 98% of cyberattacks – against businesses and otherwise – involve social engineering, making this a key trend to prepare for across the next year.
- Only 74% of companies have specific cybercrime insurance to cover losses.
- Direct premiums for cyber insurance expected to reach $23 billion in 2025.
- Firms lose up to 1.3% of their market value in the month following a cyberattack.
- By the end of the year, up to 60% of companies on supply chains will be using the risk of cybersecurity as a buying consideration when partnering with others.
- The median time between hacker access and ransomware launch is 6.11 days for assumed and confirmed attacks.
- 207 Cybersecurity Stats and Facts for 2025

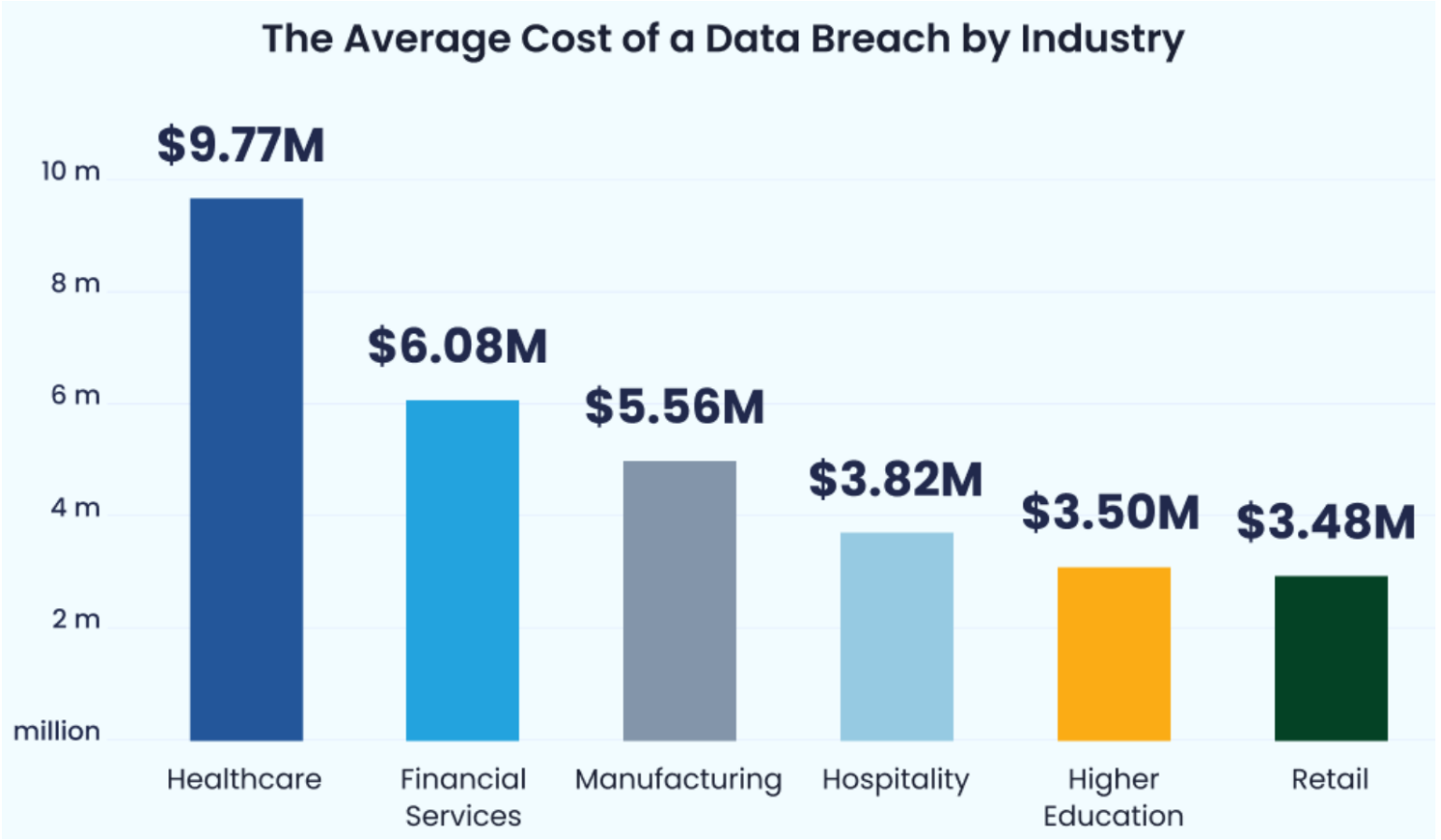
Cyber Stats and Facts 2025 continued

- 8% of cybersecurity leaders admitted they or a teammate intentionally did not report a cyber incident for fear of job loss. 30% said 2–4 incidents went unreported to executive leadership in the past year.
- Security leaders cite the top 3 reasons for not reporting a cyber incident are:



- [207 Cybersecurity Stats and Facts for 2025]

Cyber Stats and Facts 2025 continued



- [207 Cybersecurity Stats and Facts for 2025]

AI Specific Cyber Stats

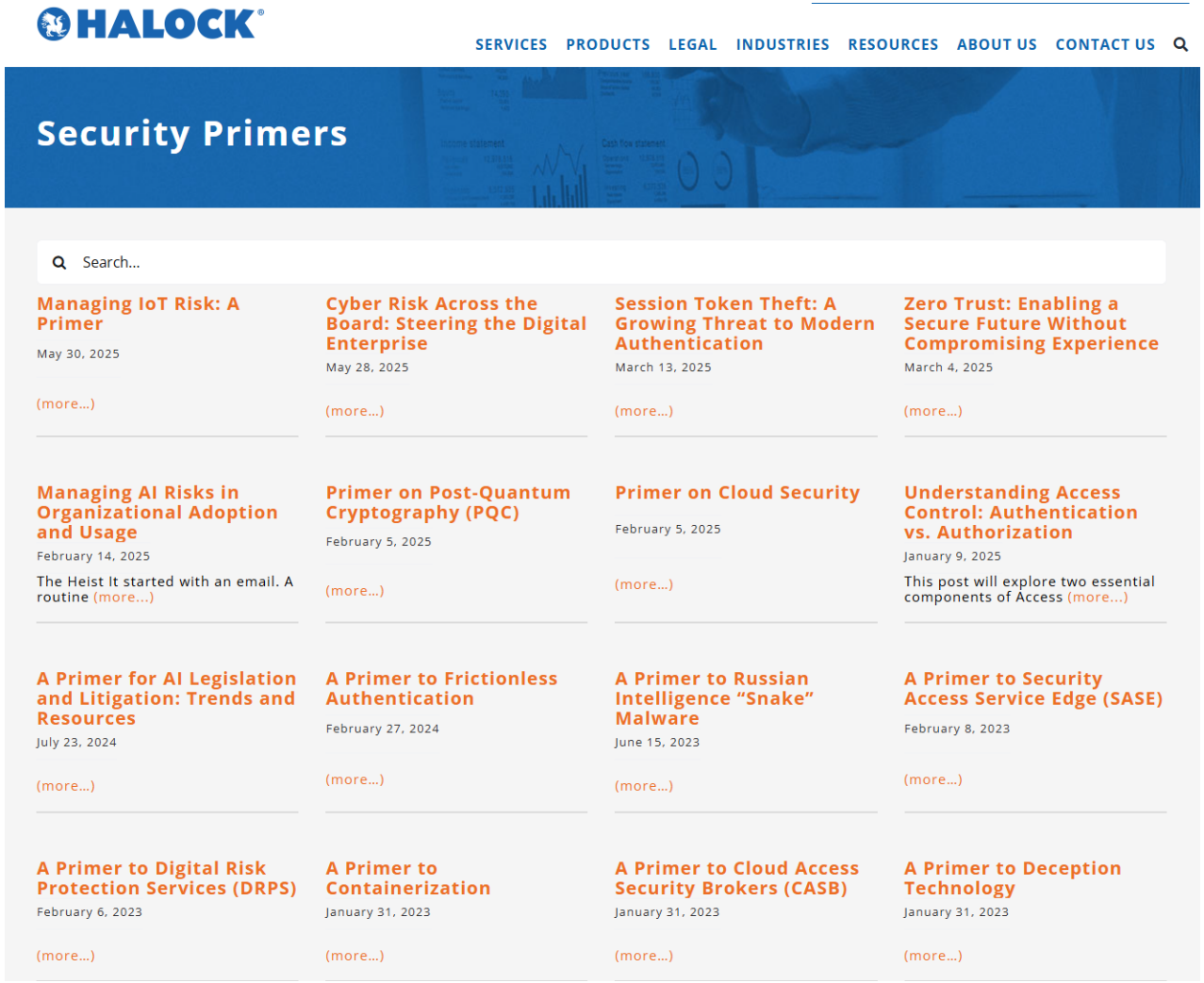
- It's estimated that 80% of phishing attacks are AI-generated.
- Companies using AI save more than $3 million per breach.
- AI cybersecurity market set to exceed $133 billion by 2030.
- 63% of companies are considering implementing new technologies, such as GenAI, to support cybersecurity employment shortages.
- Research suggests companies adopting GenAI to support hyper-personalized training could result in 40% fewer employee-caused security incidents by 2026.
- 207 Cybersecurity Stats and Facts for 2025

Briefing Agenda

- **New Security Primers**
- **Regulations and Standards Updates**
- **Industry Reports**
- **Hacker News**
- **Breach Litigation**
- **AI Risks**
- **Browser Security**
- **Continuous Exposure Management**

New Security Primers - 2025

- Trust buy Verify (Software Supply Chain Attacks) 10/08/2025
- Help Desk Social Engineering Primer 10/02/2025
- AI Native Browser Security Primer 09/19/2025
- Insurance Vertical: Security Primer 6/23/2025
- Browser Security Primer 6/17/2025
- Securing Agent 2 Agent Considering MCP 6/17/2025
- Top Threats Healthcare Vertical 6/4/2025
- Weathering the Storm with Good Cyber Governance 05/19/25
- Internet of Things 05/09/2025
- AI Plagiarism, Policy & Procedures Templates 03/21/2025
- Session Token Theft 03/13/2025
- Zero Trust 02/24/2025
- Deception Technology 02/27/2025
- AI Risk, 2/14/2025
- Cloud Security 02/03/2025
- Post Quantum Computing 01/24/2025



- [Client Security Briefing - HALOCK]

HHS OCR Risk Analysis Initiative

- OCR brought 22 enforcement actions in 2024
- Focus on the Risk Analysis provision of the HIPAA Security Rule
- Settlements in recent weeks with 4 entities that did not perform compliant risk analyses
- HIPAA regulated entities should ensure they are conducting accurate and thorough risk assessments
- Health Data Privacy & Security: A Look Back at the Final Enforcement Push From HHS Under the Biden Administration
- OCR's New Initiative Yields Seven HIPAA Enforcement Actions | Feldesman LLP

New Proposed Updates to the HIPAA Security Rule

- Require the development and revision of a technology asset inventory and a network map that illustrates the movement of ePHI
- Require greater specificity for conducting a risk analysis:
  - A review of the technology asset inventory and network map.
  - Identification of all reasonably anticipated threats to the confidentiality, integrity, and availability of ePHI.
  - Identification of potential vulnerabilities and predisposing conditions to the regulated entity's relevant electronic information systems
  - An assessment of the risk level for each identified threat and vulnerability, based on the likelihood that each identified threat will exploit the identified vulnerabilities.
- Strengthen requirements for planning for contingencies and responding to security incidents:
  - Establish written procedures to restore the loss of certain relevant electronic information systems and data within 72 hours.
  - Perform an analysis of the relative criticality of their relevant electronic information systems and technology assets to determine the priority for restoration.
  - Establish written security incident response plans and procedures documenting how workforce members are to report suspected or known security incidents and how the regulated entity will respond to suspected or known security incidents.
  - Implement written procedures for testing and revising written security incident response plans.
- Require regulated entities to conduct a compliance audit at least once every 12 months to ensure their compliance with the Security Rule requirements.
- Require vulnerability scanning at least every six months and penetration testing at least once every 12 months.
- Comment period open until March 7, 2025 but delays likely with new administration reviewing
- HIPAA Security Rule Notice of Proposed Rulemaking to Strengthen Cybersecurity for Electronic Protected Health Information | HHS.gov

Insurance in Crosshairs -06/23/2025

- Aflac (June 2025)
- Erie Insurance (June 2025)
- Prudential Insurance (February 2024)
- Change Healthcare (February 2024)
- **Tactics**: All events link back to compromised credentials, provider portals, MFA fatigue, and help-desk impersonation.
- Reliance on third-party administrators including outsourced platforms and document processors.
- **Recommend**: map third party access points, segment and monitor external access, tighten IAM, strengthen help desk verification protocols, and extend IR to vendor paths and playbooks and response procedures

FFIEC CAT is out of the Bank

- FFIEC is officially sunsetting its Cybersecurity Assessment Tool (CAT) on August 31, 2025
- financial institutions must now make the **leap from a static maturity model to continuous, risk-informed assessments**
  - **Mindset Transformation**: Security is no longer about passing audits—it's about **business-aligned risk** decisions.
  - **Cyber Risk Accountability:** Cybersecurity governance must **break out of compliance silos** and become a cross-functional enterprise discipline.
  - **Cultural Shift**: Boards and executives need to engage beyond attestation, asking how cyber risks can cause harm to the organization and to those outside of the organization.
- FFIEC encourages institutions to transition to CRI Profile, NIST CSF 2.0, and CIS Critical Security Controls
- The CAT Is Out of the Bank: A New Era in Cybersecurity

NYDFS Part 500 Updates

- Updates take effect May 1, 2025
- Must conduct "automated scans of information systems, and a manual review of systems not covered by such scans to discover, analyze, and report vulnerabilities."
- Frequency of reviews to be determined by risk assessment and promptly after material changes.
- Class A entities to implement EDR and SIEM
- NYDFS Updates Regulated Firms on Upcoming Cyber Requirements - Lexology

Regulation S-P (amendments) 05/14/2025

- Key Enhancements to Regulation S-P
- **Incident Response Program**
  - Reasonably detect, respond to, and recover from unauthorized access to customer information
- **Customer Notification Requirement**
  - Notify affected individuals whose sensitive customer information was or reasonably likely to have been accessed without authorization (not later than 30 days)
- **Third-Party Service Providers (Vendor Risk Mgmt)**
  - Written policies and procedures for oversight of service providers including those that may monitor affected individuals
- SEC.gov | Regulation S-P – Back to the Future
- 34-100155-fact-sheet.pdf

DoD Finalizes CMMC 2.0 -09/10/2025

- Cybersecurity Maturity Model Certification 2.0
  - Effective November 10, 2025 (3-year phase in)
  - Incorporated into regulation (32 C.F.R Part 170)
  - Formalizes the assessment and attestation process
  - Level 1 correlates with FAR clause requirements
  - Level 2 with NIST SP 800-171
  - Level 3 with NIST SP 800-172
  - Applies to contractors that handle FCI or CUI
- Department of Defense Finalizes Long-Awaited Cybersecurity Rule | Government Contracts Insights

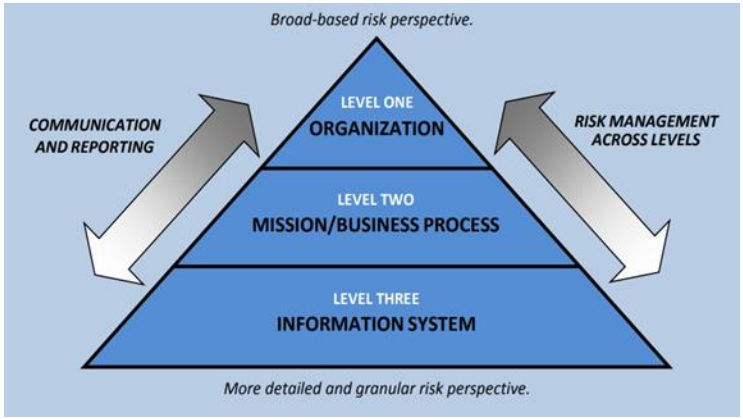
PCI DSS v4.0

- 51 new requirements move from best practice to required by March 31, 2025
  - SAD (sensitive authentication data) needs to be encrypted prior to authorization
  - Additional cryptographic controls and protocol requirements
  - Updated MFA requirements
  - Additional requirements on scripts executed on consumer browsers
  - Service Accounts to be managed (application and system)
  - Targeted risk analysis used to determine “periodic”
  - Targeted risk analysis used to address and prioritize non high-risk / critical vulnerabilities
  - Updated security awareness training requirements
  - Increased IR Plan detail and Procedures
- Emerging PCI DSS 4.0 Requirements that are Due by March 2025
- PCI Compliance Archives - HALOCK

Good Governance (brief)

05/19/2025

- Mature Cyber Risk Management
  - Executives and the entire chain of command can make informed decisions (everyone sees the same dashboard)
  - Meeting Duty of Care
  - Cybersecurity Risk Management is aligned with the business appetite
  - Adaptable: risk posture changes as the world changes
  - Good cyber governance = cyber resilience



Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies – July 26, 2023

- Think of this as Sarbanes Oxley (SOX) for Cybersecurity.
- The intent is to provide investors transparent information about cyber risk management.
- They apply to public companies registered with the SEC.
- If any of your customers are **publicly traded companies**, expect them to include you in their third-party risk management (TPRM) program.
- This will set expectations for open communication about cyber risk for all businesses.

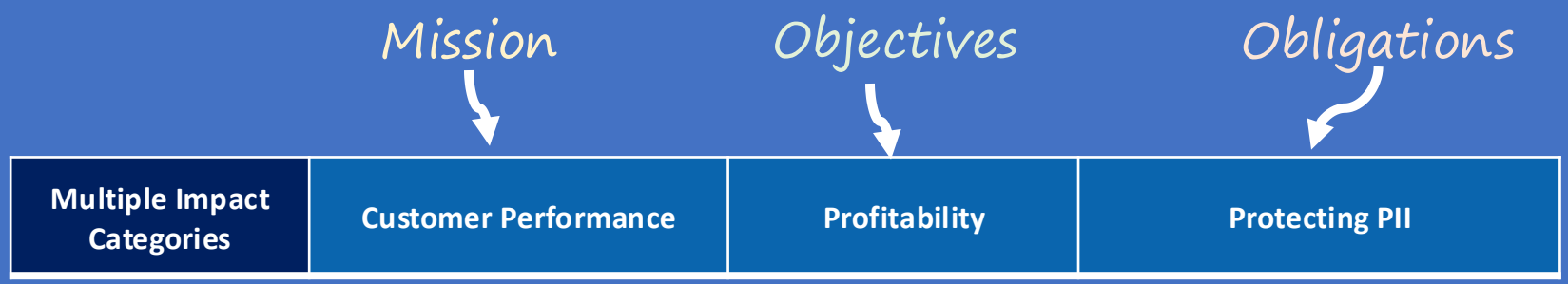
- Annual 10-K Survey 2024 - Risk Management

Cyber Insurance Continues to Evolve

- Underwriters are beginning to recognize the connection between good governance and lower liability. Proposed updates to the application below:

Factors	Question
Scope	Are all systems that pose a risk of harm to the public included in a risk assessment?
Risk analysis	Are you evaluating risks to systems and information using the likelihood and impact of threats?
Risk analysis	Is harm to parties outside of your organization an explicit factor in your risk calculation?
Risk analysis	Do you only accept risk when the risk is acceptable to both your organization and outside parties who might be harmed by those risks?
Risk analysis	Do you determine the reasonability of safeguards by comparing the costs and burdens of safeguards to the weighted impact?
Risk management	Do you have a roadmap that prioritizes the largest risks?
Risk management	Can you demonstrate that you are treating risks over time?
Risk management	Are executives participating in periodic review of cybersecurity risks and the roadmap?
Risk management	Do executives provide sufficient resources (budget, staff, etc.) to support the roadmap?

Duty of Care Risk Scoring



Identify the following to prepare risk criteria:

- Your *Mission*: Your purpose for existence.
- Your *Objectives*: Company goals and mandates.
- Your *Obligations*: The care you owe others.

Impacts using Duty of Care Risk Analysis

(example)

IMPACT	MISSION What you do for your customers	OBJECTIVES Your business goals	OBLIGATIONS Your public duty
Definition	**1. We work every day to be the leading global provider of high value, mission-critical solutions that help customers safely, reliably, and productively keep their assets moving.**	**1. To be a leading marketer and world class manufacturer of power transmission, aerospace, and specialty components, and provide superior growth** **2. To support annual operational and fiscal goals.**	**1. Protect personnel information.** **2. Protect customer information.**
Negligible	**1.00** No detected impact or impairment of mission.	**1.10** Targets set in strategic plans remain on target. **1.20** Annual operational and fiscal goals remain on target.	**1.10** CUI and customer information remains accessible only to approved parties. **1.20** Personnel information remains accessible only to approved parties.
Acceptable	**2.00** We would not expect to see customer satisfaction surveys describe a negative perception.	**2.10** Strategic plans would be off target, but within planned variance. **2.20** Annual operational and fiscal goals would be off target, but within planned variance.	**2.10** Compromise of information assets may cause concern to customers but would not result in harm. **2.20** Compromise of information assets may cause concern to personnel but would not result in harm.
Unacceptable	**3.00** Some customers would report that Acme could not help them safely, reliably, productively keep their goods and assets moving.	**3.10** Strategic plans or annual operational and fiscal goals would be off target and outside of planned variance. **3.20** This would require countermeasures to recover.	**3.10** At least one customer would experience harm (financial, safety, etc.) as a result. **3.20** A small set of personnel suffer harm such as identity theft, reputational damage, or financial harm.
High	**4.00** Many customers would report that Acme could not help them safely, reliably, productively keep their goods and assets moving.	**4.10** Strategic plans or annual operational and fiscal goals would be severely off target and would require material investment or lost opportunity to recover. **4.20** Would result in Business Unit failure.	**4.10** Multiple customers would experience harm (financial, safety, etc.) as a result. **4.20** A material count of personnel suffer harm such as identity theft, reputational damage, or financial harm.
Catastrophic	**5.00** Acme would not be able to help customers safely, reliably, productively keep their goods and assets moving.	**5.10** Acme could not operate as a profitable organization.	**5.10** Multiple customers would experience significant harm (financial, safety including loss of life, etc.) as a result. **5.20** Personnel suffering irreparable harm or loss of life.

Traits of Cyber Resilient Organizations – 05/08/2025

- LevelBlue surveyed 1,500 organizations, only 7% classified as cyber resilient
- Only 37% of organizations surveyed had incident response plans
- Cyber resilient organizations (top 7%) did not experience breach in last 12 months
  - Aligned cybersecurity and business goals
  - Business risk appetite aligned with cybersecurity risk management
  - Cybersecurity responsibility to all leadership roles
  - Cybersecurity budgeted for all new projects
  - Defending against AI powered attacks by employing AI for their own defenses
- Cyber resilience is the strategy: Why business and security must align now | SC Media

Benefits of Strong Incident Response Readiness – 05/12/2025

- Lower cyber insurance premiums
- Meet compliance *(evidence of readiness to interested parties)*
- Shorter dwell times *(identify threats faster)*
- Faster recovery times with smaller blast radius
- Reduce liability claims
- Executive involvement fosters awareness *(through tabletops)*
- Integrate cyber resilience in the lines of business

- Cyber Security Incident Readiness | Prepped for Threats & Risk

INCIDENT RESPONSE PLAN (IRP)

We help you create a detailed incident response plan, ensuring that your organization has a roadmap to follow during a security event.

TABLETOP EXERCISES FOR INCIDENT RESPONSE TEAM TRAINING

Tabletop exercises based upon your run books and custom industry scenarios to ensure personnel are familiar with your incident response plan and understand their roles.

INCIDENT RESPONSE TECHNOLOGY REVIEW

Review and assess in place security solutions and configurations that could assist with an incident or investigation.

Verizon 2025 Data Breach Investigations Report (4/2025)

- Verizon

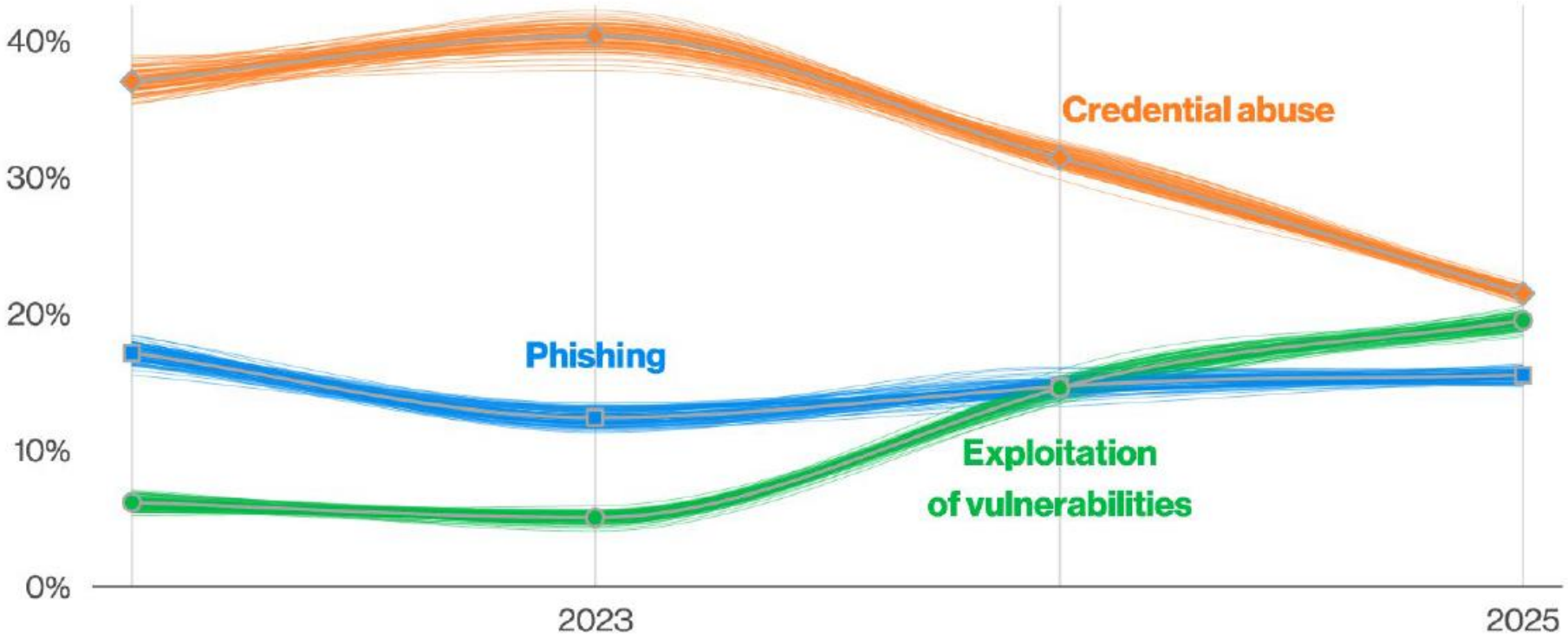


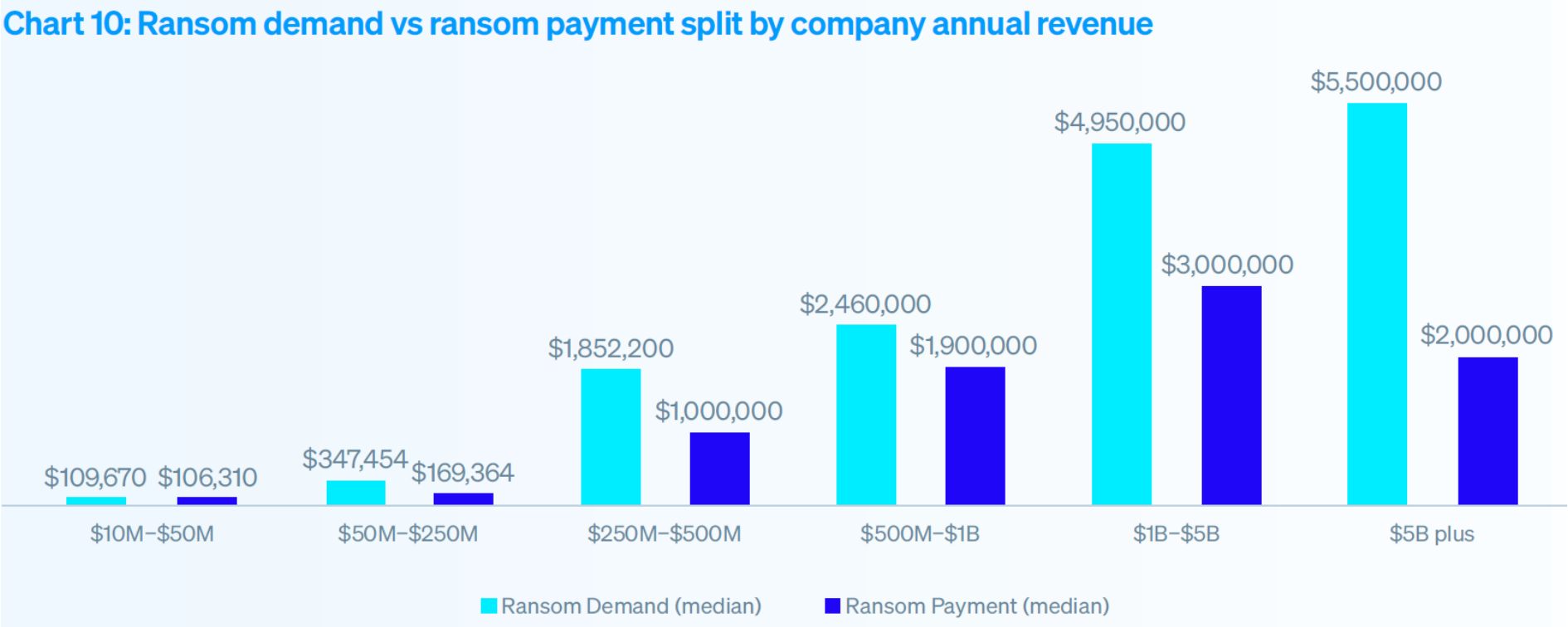
Figure 16. Known inital access vectors over time in non-Error, non-Misuse breaches (n in 2025 dataset=9,891)

Verizon 2025 Data Breach Investigations Report (4/2025)

- 22K incidents, 12K breaches, 139 countries
- Edge device vulnerability exploitation increased 8 X
- Use of stolen credentials down to 22% of breaches from 31%
- Exploiting vulnerabilities was 20% of all breaches (34% increase)
- Breaches involving Ransomware increased from 32% to 44%
- Extortion demand payments decreased from 150K to 115K
- 60% of breaches involved human element
- Third-party involvement was 30%, up from 15% previous year
- 66% of disclosed web application infrastructure secrets are JSON Web Tokens
- 43% of disclosed cloud-infrastructure secrets are Google Cloud API keys

- Verizon

State of Ransomware 2025 – 06/30/2025



- [2025 Ransomware Report: Sophos State of Ransomware]

State of Ransomware continued

- 3,400 leaders across 17 countries whose organizations were hit by ransomware
- 54% recovered using backups
- 49% paid the ransom
- Ransom demands dropped 34% to $1.3M
- Ransom payments dropped by 50% to $1M
- Cost to recover averaged $1.5M
- 53% recovered after 1 week
- Technical root cause
  - Exploiting vulnerabilities (32%)
  - Compromised credentials (29%)
- 2025 Ransomware Report: Sophos State of Ransomware

NPM Breach - 09/09/2025

- Massive software supply chain compromise
- NPM is an app store for software developers (largest supplier of code)
- **What happened?** A supply chain attack compromised the NPM account of developer qix, leading to malicious versions of dozens of high-impact packages being published.
- **What was the impact?** The combined weekly downloads of the affected packages exceed one billion, posing a significant threat to the JavaScript ecosystem.
- **What does the malware do?** The payload is a crypto-clipper that steals funds by swapping wallet addresses in network requests and directly hijacking crypto transactions.
- **How to protect yourself:** Immediately audit your project's dependencies. Pin all affected packages to their last known-safe versions using the overrides feature in package.json.

- New Security Breach Threatens Crypto And Everyday Apps
- Anatomy of a Billion-Download NPM Supply-Chain Attack
- Self-Replicating Worm Hits 180+ Software Packages – Krebs on Security

SalesLoft Drift breach – 09/05/2025

- Salesloft Drift is third-party application to Salesforce
- Drift Connected App uses AI to automate various sales processes including communications, analysis and engagement and integrates with Salesforce databases
- OAuth tokens compromised Aug 8-18, 2025
- Threat Actor UNC6395
- 700 organizations impacted including Cloudflare, Zscaler, Palo Alto, Tanium, SpyCloud
- Threat actor used stolen tokens to access email of Google workspace accounts
- Okta blocked attempt as connection originated from unauthorized IP address
- Recommend: review third party integrations with Drift instance, revoke and rotate credentials. Enforce IP restrictions on the Drift Connected App.
- Widespread Data Theft Targets Salesforce Instances via Salesloft Drift | Google Cloud Blog
- Blast Radius of Salesloft Drift Attacks Remains Unclear

Scattered Lapsus$ Returns

10/03/2025

- Threat actors Unite: Scattered Spider, Lapsus$, ShinyHunters
- Published a goodbye letter July, 2025
- Resurgence October 2025
- Vished support personnel of Salesforce clients
- Extortion demand made to Salesforce
- Not a direct Salesforce security issue
- Scattered Lapsus$ Hunters Drops Salesforce Leak Site

16B login credentials exposed in world's largest data breach 6/23/2025

- Credentials are not recycled from old breaches
- Acquired from recent infostealers (fresh credentials)
- Malware infected in approved plug-ins/extensions
- Data includes a URL, login details and password
- Many include tokens, cookies, and metadata
- Apple, Facebook, Google, and many others
- MFA a must to defend against the theft of data
- 16 billion passwords exposed in colossal data breach | Cybernews

GhostAction GitHub 09/09/2025

- Adversaries infiltrated the CI/CD environment by exploiting misconfigured credential management systems
- Attackers harvested 3,325 secrets including API tokens, configuration data, and other sensitive credentials.
- **GhostAction** malware custom developed, functioning as a stealer tool, to facilitate internal data exfiltration and maintain persistence across affected networks.
- Critical to immediately rotate and revoke all API keys, tokens, and credentials that may have been exposed as a result of the breach.
- Review the integrity of CI/CD configurations to ensure that only validated and secure sources are being used for code deployment.
- GhostAction GitHub Supply Chain Attack: Hackers Steal 3,325 Secrets from a Critical CI/CD Repository

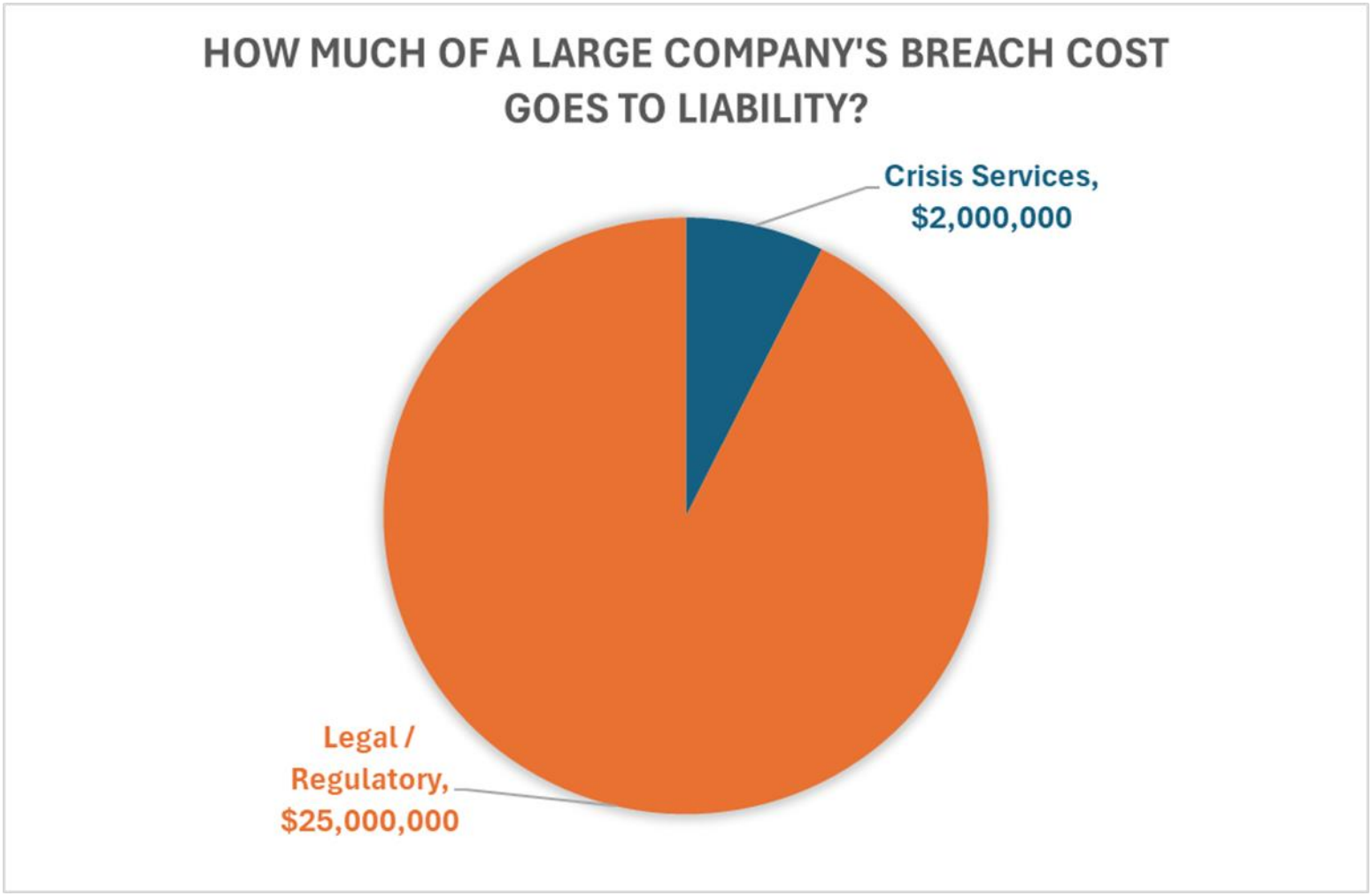
Software Supply Chain Primer 10/08/2025

- Trust based on code origin is not enough.
- Approved sources can be compromised post-approval.
- Include integrity validation in token protections.
- Verify authentication tokens at the application or API gateway level.
- Dependencies must be treated as untrusted input in CI/CD pipelines.
- Supply chain now includes developer identities and tokens.
- Depending on your risk, tighter controls including hardware-backed MFA, scoped access, and build time verification can be implemented to reduce credential abuse and limit the extent of compromise.
- Monitoring and verification must be continuous.
- CDR and SSPM integrations can be used to monitor registry, SaaS, and cloud activities to identify OAuth token abuse, privilege escalation, and mass downloads.

23andMe Bankruptcy - 04/08/25

- 2023 data breach expose 7 million customer's sensitive data including raw genotype data, health predisposition reports, and carrier-status reports
- 23andMe blamed customer's poor choice of passwords
- Threat actors used credential stuffing to gain access to 14,000 accounts
- Class Action settlement of $30 Million ($10,000 to victims of identity theft)
- Data Breach Fallout:
  - Reputation, operations, stock decline, resignation of CEO and co-founder, fines
  - Bankruptcy announced on March 23, 2025
- Underscores the pressure companies face when they fail to adequately protect the very data their businesses are build on
- UK watchdog fines 23andMe for 'profoundly damaging' data breach
- Regeneron Enters into Asset Purchase Agreement to Acquire 23andMe® for $256 Million; Plans to Maintain Consumer Genetics Business and Advance Shared Goals of Improving Human Health and Wellness | Regeneron Pharmaceuticals Inc.
- 23andMe Settles Data Breach Lawsuit for $30 Million
- 23andMe's Bankruptcy Highlights Extreme Cyber Risks in the Digital Age

The Cost of a Breach – 05/08/2025



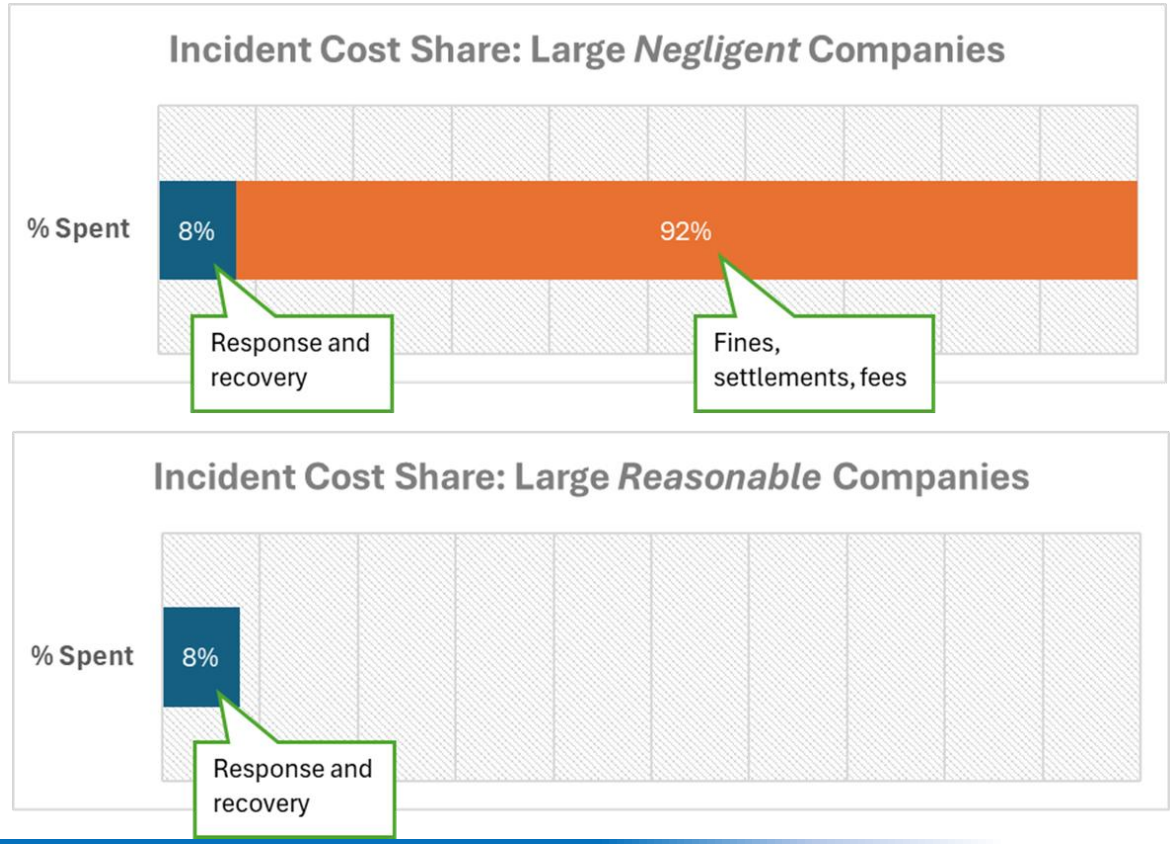
Your Security assessments may be increasing your risk!

Who sets the price on liabilities? (Fines, Fees, Settlements)

Lawyers when they negotiate settlements and try cases!

Can you speak the language of attorneys and executives?

Can you demonstrate …. Reasonability?



The incriminating evidence

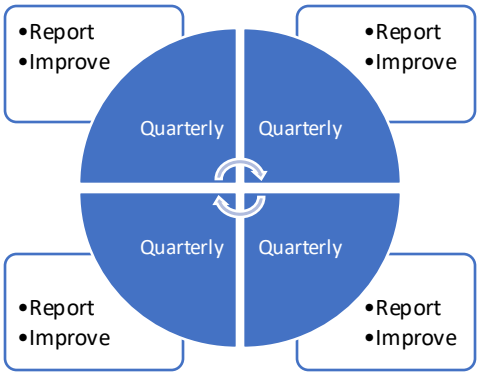
Please present your risk assessment

What the regulators are looking for: Cybersecurity Governance & Strategy

Cybersecurity Strategy and Planning

Continuous Cybersecurity Oversight

Cybersecurity Strategy	Risk Assessment	Risk Treatment Roadmap
• Business requirements • Your duty of care • Your risk criteria • Your risk appetite • Scope of governance • Cyber Governance Charter	• Risk = Likelihood x Impact • Quantify incidents at peers • Assess your preparedness • Assess risks • Reasonable remediation plan	• Remediation budget • Detailed plan • Metrics for success • KRIs for effectiveness

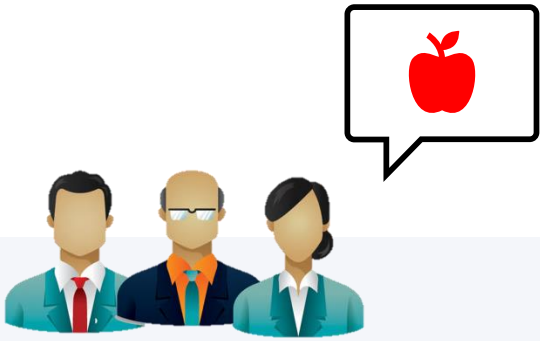


- Report business risk
- Understand status
- Informed decisions
- Evidence of governance

Cybersecurity Risk From the Executive Perspective

Why is Governance Rising as a Cybersecurity Issue?

In breach case after breach case, we see cybersecurity teams unable to communicate with executives.



EXECUTIVES

- Don't know what they should know.
- Do not understand cybersecurity personnel.

MANAGEMENT

- Does not feel comfortable being honest about risks.
- Does not know how to conduct risk analysis in business and legal terms.

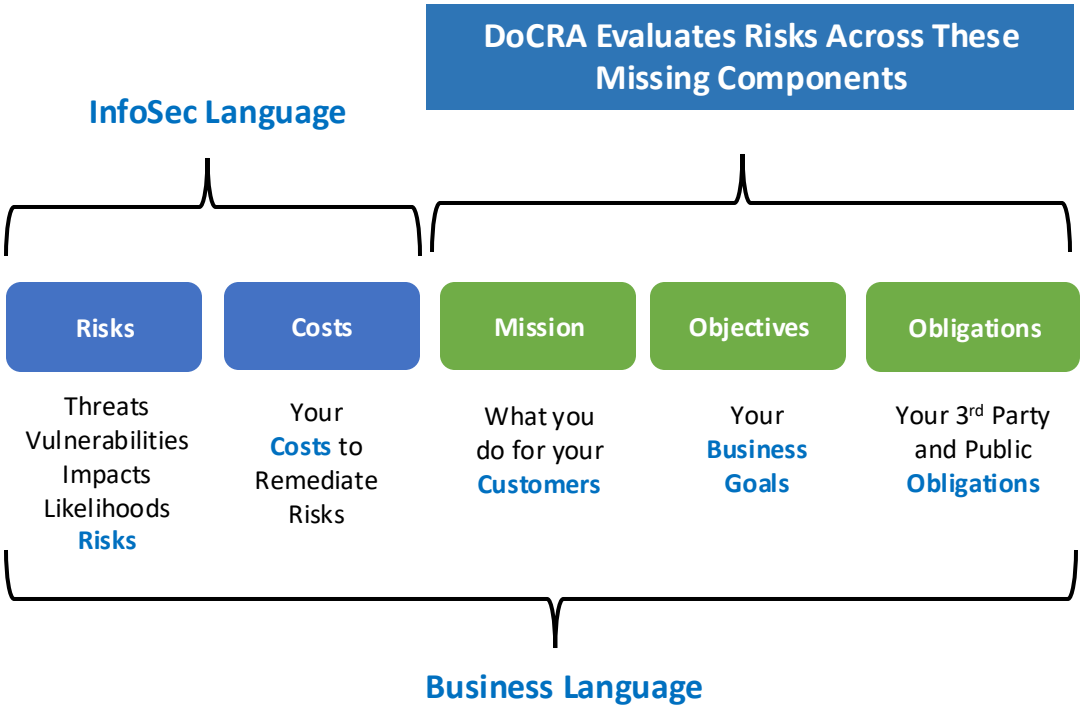
Good governance would fix this.
Good governance is good for cybersecurity.

DoCRA Creates a Common Language between Cybersecurity and Leadership (DoCRA.org)

Information Security speaks in *risks and costs*.

Business speaks in terms beyond *risks and costs*.

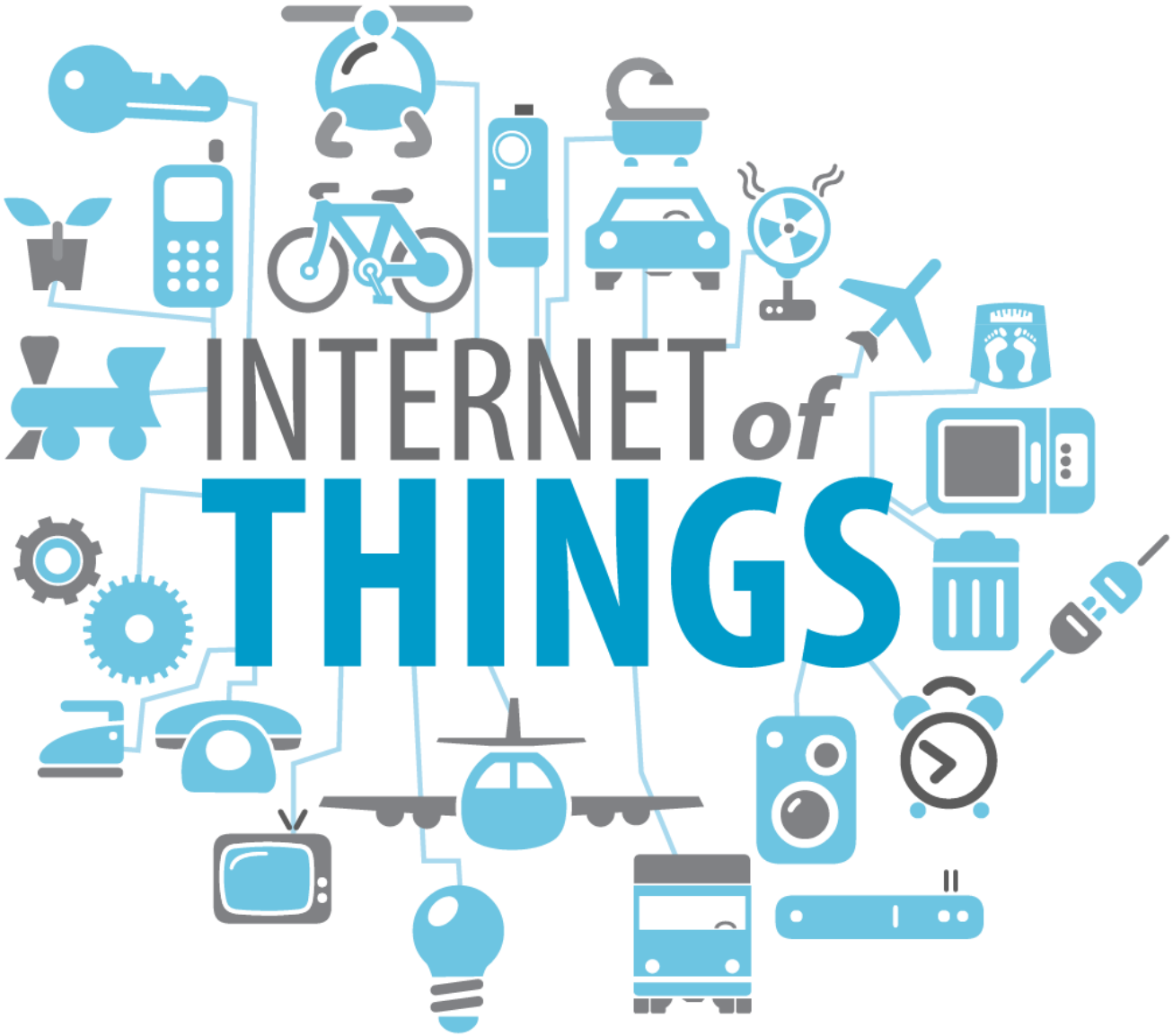
DoCRA fills in the missing components to create a common language as a universal translator.



Risk Methods based on DoCRA available:
CIS RAM v2.1 for Implementation Group 2 (IG2)

CISA Warns of Cyber Threats to Operational Technology – 05/06/2025

- CISA, FBI, EPA, and DOE warn of attacks on operational technology (OT) with recommendations
- Remove OT connections to the public internet
- Change default passwords
- Secure remote access to OT networks
- Segment IT and OT networks
- Practice the ability to operate OT systems manually
- Primary Mitigations to Reduce Cyber Threats to Operational Technology | CISA


INTERNET of
THINGS

IoT Primer – 04/17/2025

- **Industries most impacted**: Healthcare, Hospitality, Manufacturing, and Rail
- IoT systems are not peripheral, they are central to operations
- IoT ecosystems typically bypass traditional IT governance
- Unique risks with IoT
  - Long device lifecycles
  - Wide variety of hardware and communication protocols
  - Always on and often unmanaged or vendor controlled
  - Deep integration with core operations
  - 1 in 5 devices have the default password
  - Limited interface and shipped with hardcoded credentials
  - Outside of IT governance model
- Managing IoT Risk: A Primer – HALOCK
- Is IoT Finally Secure? What 2025 Taught Us About Cyber Risk in Connected Devices - IoT Breakthrough Awards

IoT Threat Vectors

Threat Vector	Description	Impact	NIST SP 800-53 Rev. 5	CIS Controls v8
Weak or Default Credentials	Devices ship with factory-set usernames and passwords that are rarely changed.	Easy unauthorized access; initial foothold for attackers.	IA-5 (Authenticator Management), AC-2	CIS Control 5.3, 6.3
Lack of Patching/Firmware Updates	Devices lack automated or manageable patching mechanisms.	Exploitation of CVEs; long-term persistence.	SI-2 (Flaw Remediation), CM-11	CIS Control 7.4, 12.6
Insecure Communication Channels	Unencrypted or poorly secured protocols (e.g., HTTP, Telnet, RF).	Data interception, manipulation, or replay attacks.	SC-12, SC-13, SC-28, SC-40	CIS Control 13.1, 13.7
Insider Threats & Physical Access	Devices are often accessible in uncontrolled environments (e.g., guest rooms, public terminals, plant floors).	Circumvents logical controls; difficult to trace.	PE-3, PE-6, PE-18, AC-6	CIS Control 14.1, 4.6
Supply Chain Exploitation	Compromised firmware, poorly vetted vendors, or vulnerable third-party components.	Backdoors or insecure defaults introduced upstream.	SR-3, SR-5, SR-6, SR-11, SR-12	CIS Control 15.1, 15.3, 16.11
Lack of Network Segmentation	Devices are placed on flat networks with unrestricted lateral access.	Escalation from low-value IoT to sensitive systems.	SC-7, SC-7(12), AC-3, AC-4	CIS Control 3.4, 13.3
Blind Spots in Monitoring	Lack of logs, telemetry, or integration with SIEM or behavioral analytics.	Delayed detection; inability to baseline or investigate.	AU-6, CA-7, SI-4	CIS Control 8.2, 8.7, 6.7

Marriott Settlement (52M)

- Multi-district (49 states plus DC)
- Settlement mandates incorporating zero-trust principles
- Also requires data minimization and disposal requirements
- Increased vendor risk management requirements
- Risk Assessments must address "harm to others"
- Iowa to receive $594,105 from the settlement
- Illinois to receive $2.1 million from the settlement
- Attorney General Bird Announces $52 Million Multistate Settlement with Marriott for Data Breach that | Newsroom | Iowa Attorney General

Zero Trust Architecture – Feb 28th, 2025

Tenets of Zero Trust (adapted from NIST 800-207)

All data sources and computing services are considered resources. Every device, application, and data source must be treated as a potential security risk and be protected accordingly.

All communication is secured regardless of network location. No implicit trust is given based on whether a device or user is inside or outside the traditional security perimeter.

Access to individual enterprise resources is granted on a per-session basis. Authentication and authorization are continuously enforced, ensuring that trust is never assumed.

Access decisions rely on dynamic policy enforcement. Policies should be based on observable data points, including user identity, device security posture, and behavioral attributes.

The organization continuously monitors and assesses the security posture of all assets. Devices and applications are regularly evaluated for vulnerabilities, with access dynamically adjusted as necessary.

Authentication and authorization are strictly enforced before granting access. This applies to all interactions, ensuring that security policies are consistently applied across the organization.

Organizations collect and analyze security data to improve threat detection. Continuous monitoring of access patterns and security incidents allows for rapid threat detection and response.

- **Solutions: MFA, Microsegmentation, SASE**
- Zero Trust: a Secure Future Without Compromising Experience

AI Phishing hits Skynet Moment – 04/03/2025

- In 2023 AI crafted phishing campaigns were 31% less effective than human red teams
- March 2025 AI is now 24% more effective than humans
- Research performed by Hoxhunt researchers
- Once integrated into Phishing-as-a-Service platforms, success ratios will rise to that of targeted spear phishing
- AI phishing hits its Skynet moment as agents outperform human red teams - SiliconANGLE

HALOCK AI Risk Primer - 2/20/2025

Application or Function	AI Hierarchy Applied AI	ML	DL	LLM/GAN*	GenAI	AgenticAI
Predictive Maintenance	■	■				
Fraud Detection	■	■				
Yield Optimization	■	■				
Malware Classification	■	■				
Crowdstrike Automated Incident and Response	■	■				
Image Recognition	■	■	■			
Object Detection	■	■	■			
Chatbots and voice assistants	■	■	■			
Handwriting Recognition	■	■	■			
Speech Recognition	■	■	■			
Natural Language Processing*	■	■	■	■	■	
ChatGPT	■	■	■	■	■	
DALL-E	■	■	■	■	■	
Gemini	■	■	■	■	■	
Github Copilot	■	■	■	■	■	
X.ai Grok	■	■	■	■	■	
Crowdstrike Charlotte	■	■	■	■	■	■

*Neural Network Type - other generative types include: GAN, VAE, Diffusion Models, NST, and Transformers (LLM)

- Managing AI Risks in Organizational Adoption and Usage

AI Risk Factors

- **AI Creep**: AI enhanced applications may transmit sensitive or proprietary data to AI models, raising privacy concerns and regulatory risk.
- **Use of AI External Devices**: use of these external tools such as ChatGPT or Copilot may leak confidential information unintentionally. AI services may not meet the organization's security standards.
- **Legal Risks**: AI generated content may not be owned by the organization. AI models may also be deemed illegal for use in certain territories or industries.
- **Exploiting AI Vulnerabilities**: Attackers can manipulate the LLM agent to extract personal information from a conversation with chatbots. AI powered coding assistants my introduce security vulnerabilities or malware into software. Threat actors can leverage AI models to create sophisticated malware to evade traditional security measures.

MCP is like API for AI - 06/04/2025

- **Model Context Protocol** (MCP) is the universal adapter for AI
- **Traditional APIs:**
  - Stateless: Each request is independent, like a one-off conversation.
  - Resource-Oriented: Designed for specific tasks (e.g., retrieve customer record, update database entry) focused on CRUD (Create, Read, Update, Delete).
  - Human-Designed: Built for predictable, programmed interactions, usually between applications or users with clear intentions.
  - Security Model: Secure with authentication per request, rate limiting, input validation, monitoring for abuse.
- **Model Context Protocol (MCP):**
  - Stateful: Maintains session context, remembering the conversation or workflow across multiple interactions. This is crucial for AI systems performing a series of tasks.
  - Capability-Oriented: Instead of specific resources, MCP provides AI with tools or capabilities (like accessing a file system or querying a database) that can be used dynamically based on the conversation's context.
  - AI-Optimized: Built for the unpredictable, dynamic behavior of AI systems that make requests based on natural language or complex reasoning.
  - Security Model: Uses session-based security with dynamic capability grants, meaning AI gets temporary access to specific tools/data based on its needs at that moment.

- There's a New AI Attack Surface You Can't Afford to Ignore: Model Context Protocol (MCP)!

MCP and MCP Server

- Dynamic Authorization will make access control tricky
- Stateful nature means we are securing an entire conversation thread spanning multiple systems and data sources
- Anthropic has released prebuilt MCP gateway servers with readied integration to popular systems (Slack, Google Drive, files systems, email, etc)
  - These prebuilt MCP gateways can be used to enforce access controls and monitor interaction
  - Stateful nature will allow organizations to track what AI accesses during a session to spot anomalies and hacking
  - MCP is capable of granting specific, tightly controlled capabilities

Specific MCP Server Risks – 06/04/2025

- MCP Servers are a single point of failure and may store Oauth tokens and other credentials for many services making MCP Server a high prize target
- Prompt Injection Attacks
- Malicious MCP server could be added to AI System and leak sensitive data (SSH Keys, API Tokens, etc)
- Dynamic capability combining tools with unpredictable outcomes and associated risks
- Weak Authorization Token Pass-Through
- Lack of built in Security Controls

AI Risk (Agent-to-Agent) 6/3/2025

Inter-agent communication presents the following primary contributing factors to risk:

- **Agent Spoofing and Impersonation:** Without authentication standards, malicious actors can inject unauthorized agents into an agent network, impersonating trusted entities to gain access, manipulate workflows, or exfiltrate data.
- **Prompt Injection Across Agent Chains:** Attackers can craft prompts or outputs that exploit trust between agents. A compromised or manipulated upstream agent may send misleading instructions to downstream agents, triggering erroneous or unsafe actions.
- **Data Leakage Through Chained Requests:** Autonomous agents can often pass sensitive inputs or intermediate results between each other. If communication is not encrypted or access-controlled, proprietary information may be exposed during transmission.
- **Lack of Auditable Decision Trails:** In distributed multi-agent environments, actions taken as a result of collective decision-making can become opaque. Without message signing and traceability, it is difficult to assign responsibility or verify the integrity of decisions.
- **Cascading Failures in Coordinated Tasks:** A failure or compromise in a single agent can cascade across dependent agents, leading to systemic failures in automated workflows or decision pipelines.

Managing AI Risk – Feb 13, 2025

1. **Conduct an AI Inventory –** Identify all AI-powered applications, external AI services, and internally developed AI models in use within the organization. Add this to your CMBD.
2. **Assess Data Exposure Risks –** Evaluate what data AI systems access, store, and process, ensuring compliance with data privacy regulations.
3. **Implement AI Usage Policies –** Define acceptable AI use cases, including guidelines on data input, access controls, and employee responsibilities.
4. **Establish Vendor Risk Management –** Review AI-related security and compliance risks when engaging third-party AI providers and document contractual safeguards.
5. **Monitor AI-generated Outputs –** Regularly audit AI-driven content, decisions, and recommendations to detect biases, errors, or security risks.
6. **Secure AI Against Cyber Threats –** Implement protections against adversarial AI attacks, prompt injections, and deepfake-based fraud.
7. **Train Employees on AI Security Risks –** Educate staff on AI-related threats such as deepfake scams, AI-generated phishing, and data leakage risks.
8. **Ensure Legal & Regulatory Compliance –** Stay updated on AI regulations across different jurisdictions to avoid legal and compliance pitfalls.
9. **Define Incident Response for AI Breaches –** Develop a response plan for AI-related security incidents, including fraud, misinformation, or data exposure.
10. **Continuously Reevaluate AI Risks –** Regularly review and update AI risk assessments to address emerging threats and technological advancements. Integrate into IT risk management processes as another risk to manage.

Third-Party AI Risks 6/3/2025

The primary contributing factors to risk associated with third-party AI include:

- **Opaque AI Usage:** Vendors may not disclose their use of AI systems, how these systems are trained, or the underlying data sources. This lack of transparency hinders due diligence and risk assessment, increasing exposure to unintended consequences or liabilities.
- **Cascading Failures:** When a third party's AI malfunctions, such as a logistics partner's route optimization tool producing erroneous outputs, it can trigger downstream operational disruptions that affect customer service, compliance timelines, or financial performance.
- **Regulatory Misalignment:** Vendors operating in different jurisdictions may use AI in ways that conflict with local data protection laws or industry regulations. Organizations relying on these vendors may become non-compliant by proxy.
- **Audit and Control Limitations:** Organizations often lack visibility or contractual rights to audit or validate the performance, security, or ethical compliance of third-party AI systems, leaving them vulnerable to blind spots and hidden exposure.
- ISO/IEC 42001:2023 - AI management systems

ISO 42001:2023

6/3/2025

- AI Management System should be integrated with the organization's processes and overall management structure. Examples of management processes:
  - determination of organizational objectives, involvement of interested parties and organizational policy
  - management of risks and opportunities
  - processes for the management of concerns related to the **trustworthiness of AI systems such as security, safety, fairness, transparency, data quality and quality of AI systems throughout their life cycle**
  - processes for the management of suppliers, partners and third parties that provide or develop AI systems for the organization
- ISO/IEC 42001:2023 - AI management systems

Possible AI Vendor questions – Dec 16, 2024

1. Is AI used in the delivery of your services? (Y, N)
2. What is the intended use case of the AI model?
3. What type of AI technology is being used (e.g. machine learning, deep learning, neural networks)?
4. What data sources are used to train the AI model?
5. How is data privacy managed within AI system?
6. How is data pre-processed and cleaned before AI model training?
7. Do you overview your AI for current regulations? (e.g. weekly, monthly, quarterly)
8. What measures are in place to protect sensitive data used in training and operation?
9. How is data anonymization or pseudonymization handled?
10. How is user privacy considered when interacting with the AI model?
11. How is the AI Model tested for potential biases in the training data?
12. What mechanisms are in place to detect and mitigate adversarial attacks?
13. What is the process and how frequently do you use the process for updating and re-training the model to address emerging threats?
14. How is the model's performance monitored and evaluated for accuracy and reliability?
15. Where is the AI model deployed, and what security controls are in place at that location?
16. What mechanisms are used to monitor the AI model for unusual behavior or potential security issues?
17. How are alerts and incidents related to the AI model investigated and responded to?
18. Does the AI system comply with relevant data privacy regulations (e.g. GDPR, CCPA)?
19. What policies and procedures are in place to manage the ethical use of AI?
20. How is the AI system being monitored for compliance with industry standards best practices?

ISO 23894: Risk Management for AI

- Similar content as NIST AI RMF Playbook - AIRC
- Identify, manage and treat AI-specific usage risks
  - Bias/fairness, data quality, transparency
  - Security vulnerabilities
  - Ethical concerns and misuse
- Help organizations balance AI innovation benefits against potential harms
- Promote accountability
- Increase trust among users, regulators, and society
- OVE/ONORM EN ISO/IEC 23894:2024 - Information technology - Artificial intelligence - Guidance on risk management (ISO/IEC 23894:2023)

ISO 42001 vs ISO 23894

- ISO 42001
  - Designed for AI system providers (AI ISMS)
  - Holistic approach to AI systems: risks, ethics, governance
  - Focus on broader AI governance and operational objectives
  - Aligns with ISO 27001 PDCA
  - Certification available, e.g. Anthropic, AWS, Synthesia
- ISO 23894
  - Adopted internally for management AI related risks
  - Designed for organizations that may deploy and use AI systems
  - Focused more on security vulnerabilities and adversarial tasks
  - Emphasizes ongoing risk monitoring and treatment
  - Can guide other risk management processes
  - Aligns with ISO 31000 general risk management

Bankruptcy Court Sanctions Lawyer for Relying on AI-generated Legal Research–07/18/2025

- Marla C. Martin Case No 24 B 13368
- Four Cases referenced by debtor counsel relied on for the argument were fabricated by AI
- "*none of them exist as alleged in brief. Worse still, none of the quotations relied upon in the brief are actual statements written by any court.*"
    - Judge Michael B. Slade (Northern District of IL)
- Debtor counsel said he "*assumed that an AI program would not fabricate quotes entirely*."
- Rule 11 requires attorneys to confirm the existence and validity of legal authorities by which they rely.
- In-re-Martin.pdf
- Bankruptcy Court Sanctions Lawyer for Relying on AI-Generated Legal Research - Lexology

AI Copyright Infringement Lawsuit Anthropic Case – 09/11/2025

- Anthropic Agreed to pay USD 1.5 billion (3k each work)
- Court assessed that there was no violation of fair use for the training model itself, it was the unauthorized collection and storage of copyrighted works at issue.
- Recommendations:
  - Ensure the legality of data sources
  - Work only with reliable suppliers
  - Develop a structured policy for training with copyrighted works
  - Include strong contractual protections with suppliers
  - Develop technical capabilities to filter copyrighted content
- Landmark Settlement in AI Copyright Infringement Lawsuit - Anthropic Case - Lexology

AI Incident Sharing Initiative MITRE ATLAS – October 8, 2024

- MITRE Announces AI incident Sharing Project
- Part of MITRE's Adversarial Threat Landscape for Artificial Intelligence Systems (ATLAS) framework
- Safe place to share and collaborate AI focused attack techniques
- Must share data to be considered a trusted member to receive
- MITRE ATLAS: MITRE ATLAS™: Incident Sharing

HALOCK HACKER INSIGHT – 4/8/2025

Vulnerable Legacy Broadcast Protocols

- Legacy protocols including Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) are vulnerable to man-in-the-middle attacks
  - Discover protocols and absence of SMB messaging signing
  - Trick requesting device
  - Capture Credentials (NetNTLM hash)
  - Offline brute-force of hash
  - Full access
- Lesson 1: Disable LLMNR and NBT-NS
- Lesson 2: Enforce SMB Message Signing
- Lesson 3: Enable LDAP Channel Binding and EPA
- Lesson 4: Use SIEM to monitor for excessive LLMNR and NBT-NS queries
- Exploiting API Endpoints

Session Token Theft (HOW) – 03/13/2025

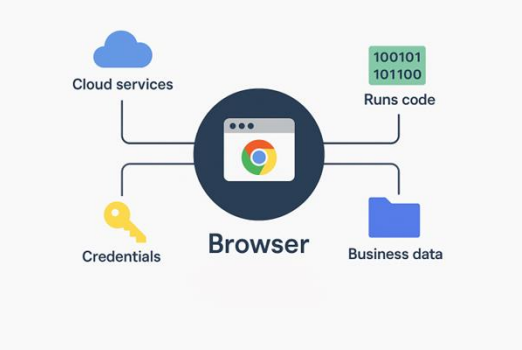
- How it happens:
  - Phishing
  - Session Fixation
  - Malware, Infostealers
  - Man-in-the-middle attacks
  - Session Replay Attacks
  - Browser Exploitation
  - Cloud Attacks
  - Compromised Primary Refresh Tokens
  - Session Token Theft: A Growing Threat to Modern Authentication - HALOCK

Session Token Theft (the fix) – 03/13/2025

- Mitigation Strategies:
  - Phishing resistant hardware-backed Auth (FIDO2/WebAuthn)
  - Adopt short lived session tokens
  - Continuously validate tokens
  - Implement refresh token rotation
  - Implement Zero Trust Network Access
  - Primary Refresh Token Protection
    - Bind to devices, continuous access evaluation, conditional access
  - Browser Protection
    - Limit session storage, EDR to detect infostealers,
  - Development Best Practices
    - Implement secure Oauth 2.0 and OpenID Connect flows
    - Prevent token leakage (never expose tokens in logs, URL, headers, etc)

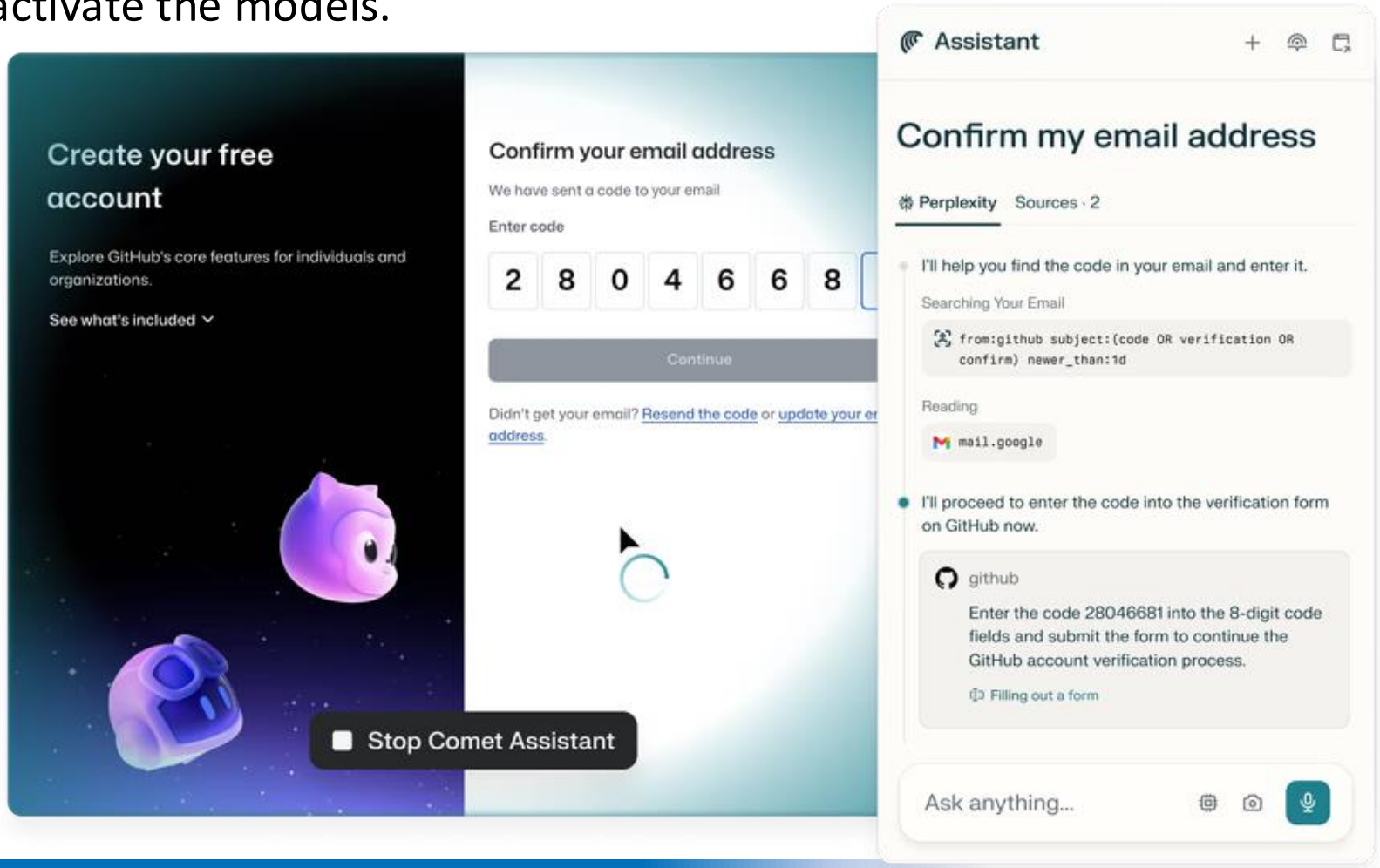
Browser Security Primer

- The Challenge
  - Extensions and plugins can pose a security risk of infostealers being installed
  - Browser policy enforcement is fragmented
  - Tooling is an issue
  - Browser behavior is security blind spot
- Securing the Browser
  - Standardized Browser Configuration Settings
    - CIS Downloads (see Desktop Software section)
    - Disable password storage
    - Block third party cookies
    - Enforce safe browsing and sandbox modes
    - Limit plugin and Javascript execution
  - Control Extension installation (approved list)
  - Monitor and assess Extension Behavior (LayerX, SquareX, others)
  - Secure Enterprise browsers (Island.io)



AI Native Browsers

An AI browser is a web browser that is built from the ground up with AI at the core of the user experience, and no user intervention is required to activate the models.



AI Native Browser Primer -09/19/2025

- Data Leakage and Unintentional Exposure
- Loss of Observability (*operates inside the rendering layer that existing tooling cannot see*)
- Malicious Extension Risk
- Manipulation and Prompt Injection
- Compliance and Policy Evasion (*downloading unapproved content, sending prompts to external APIs, output becomes flagged as AI generated*)
- **Additional Considerations for Vendors**: What are the expanded boundaries with AI Native Browser usage, policy and regulatory alignment, threat of Shadow AI
- **Practical Steps**
  - What is your current visibility of what is happening inside the browser?
  - Does the browser store and retain session context across tabs or restarts?
  - Are prompts or content sent to third-party APIs?
  - Have you applied Role-based access controls specific for AI?
  - Do you have the ability to monitor your vendor's use of AI tools?
  - Consider defining acceptable AI Interactions per workflow.
  - Create AI usage and prompt audit trail.

What is CTEM?

07/28/2025

Continuous Threat Exposure Management

- Proactive cybersecurity approach that continuously assesses, prioritizes, and addresses threat and vulnerabilities across and organization's digital environment
- 5 Gartner Steps
  - **Scoping**: identify assets, attack surfaces and systems
  - **Discovery**: continuous scanning for vulnerabilities, misconfigurations, credential exposure, and attack paths
  - **Prioritization**: Rank threats and exposures by business impact, exploitability and adversary behavior
  - **Validation**: Test exposures through simulated attacks and validate security controls and detection is working
  - **Mobilization**: Coordinate with teams to remediate findings and provide lessons learned to GRC
- What is Continuous Threat Exposure Management? | ULTRA RED Blog

CTEM Market – 09/05/2025

Problem statement: **Companies are struggling with prioritizing patch management. There are hundreds of vulnerabilities in Critical and High severity categories, which assets should I address with priority?**

Current gap: **Vulnerability scanning solutions do not have insight into the criticality of an asset to the company or if a vulnerability can be exploited with the current security controls in place..**

The answer: **Use a solution that provides the ability to provide the following:**

- Asset Discovery
- Identify Vulnerabilities
- Set asset priority /risk
- Determine if a vulnerability is exploitable and provide evidence
- Allow for continuous scanning
- Provide contextual vulnerabilities that prioritize what to remediate within rating categories (Critical, High, Medium, etc.)

Vulnerability Comparison Matrix

Features	Vulnerability Scanning	Risk Based Vulnerability Scanning (RBVS)	Continuous Threat Exposure Management	Automated Penetration Testing	Manual Penetration Testing
Asset Discovery	Partial – seeded with IP address ranges	Partial – seeded with IP address ranges	Full – Uses Top level domains to crawls for assets and IP address ranges	Partial – seeded with IP address ranges	Partial – seeded with IP address ranges
Vulnerability Scoring	Yes	Yes	Yes	Yes	Yes
Risk Based Threat Severity Ratings	No	Yes	Yes	Partial	No
Continuous Scanning / Remediation Verification	Yes	Yes	Yes	On demand – not intended for continuous scanning	Typically is a one-time RV
Validated Vulnerabilities	No	No	Yes	Yes	Yes
Remediation Guidance	Yes	Yes	Yes	Yes	Yes
Network Testing (External)	No testing	No testing	Yes	Partial – depends on vendor	Yes
Network Testing (Internal)	No testing	No testing	YES	Yes	Yes
Web Application Testing	Yes – Requires credentials	Yes – Requires credentials	Yes	Partial – depends on vendor	Yes – More granular testing

Social Engineering the Service Desk

10/02/2025

- **Practical identity proofing steps for service desks:**
  - If using knowledge-based questions, ***refrain from using knowledge-based questions that can be researched online*** or are known by others.
  - Implement self-service passwords reset functionality to avoid social engineering altogether.
  - Verify ID using a different channel that is already on record, such as a portal push, trusted callback number, or a stored manager contact.
  - Record all service desk interactions. Log all resets.
  - Privileged account escalation: Requests involving executives, IT, or admin accounts should be treated as high-risk. Require a second approver before any change.
  - Provide staff with refusal language and enable them to use it.
  - Test service desks routinely with simulated calls and reward staff who catch and stop them. Celebrate their success.
- **Two-Approver Workflow with Vendor Validation** **(see primer)**

DoCRA Resources

Video Links by Role (< 2 min)

- For Risk Managers: DoCRA for Risk Managers
- For Cybersecurity Professionals: DoCRA for Cybersecurity
- For Executives: DoCRA for Executives
- For General Counsel: DoCRA for General Counsel
- For Auditors: DoCRA for Auditor
- For Regulators: DoCRA for Regulators

Standards and Methods Links

- DoCRA Standard: The DoCRA Standard – DOCRA
- Download CIS RAM: CIS Risk Assessment Method (RAM) v2.1 for CIS Controls v8

Thank you!

Terry Kurzynski

CISO Advisor

www.halock.com

www.reasonablerisk.com

terryk@halock.com

312.391.6075

https://www.halock.com/client-security-briefing/security-primers/