Incident Response and Cybersecurity Risk Management in AI Powered Financial Systems

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

1

Incident Response and Case Studies in AI-powered Cybersecurity

CYC2/25/W1

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

2

"A breach alone is not a disaster, but mishandling it is."

—Serene Davis, Global Head of Cyber, QBE Insurance

Source: Forbytes. (n.d.). *Why Solid Supply Chain Cyber Security Is Crucial Today*. Retrieved from https://forbytes.com/blog/supply-chain-cyber-security/

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Learning Objectives

- Evaluate the role of financial professionals in incident response planning and execution
- Analyze real-world cybersecurity incidents to identify lessons for organizational improvement
- Apply frameworks such as the NIST Cybersecurity Framework to practical scenarios
- Collaborate effectively with IT and legal teams during cybersecurity crises
- Develop strategies for integrating incident response lessons into proactive risk management

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Evaluate the role of financial professionals in incident response planning and execution

Image generated by OpenAI's DALL·E through ChatGPT

5

Why Cyber Incidents Are Business Events Not Just IT Issues

Cyber breaches affect revenue operations, reporting obligations, and customer trust	Business disruptions in systems like payroll, invoicing, and ERP can halt operations Incident timelines often intersect with financial reporting cycles, leading to audit delays or missed disclosures
Finance leaders are accountable for quantifying and disclosing financial risk	Cyber incidents must be assessed for materiality and financial impact The CFO is frequently required to brief the board, auditors, and external stakeholders
Modern breaches may trigger regulatory scrutiny beyond IT scope	Finance teams often manage the broader impact from financial reporting to customer notifications and vendor communications Breaches increasingly result in restatements, fine exposure, or investor actions

SURGENT ACCOUNTING & FINANCIAL EDUCATION

6

How the Role of Finance Has Evolved in Cyber Incidents

Finance has shifted from a support function to a co-leader in response planning	Financial professionals must understand risk posture and compliance implications	Finance is a key stakeholder in disclosure and stakeholder communications
▪ Incident response budgets, insurance claims, and customer reimbursements must be finance-driven ▪ Finance often steers the cost/benefit analysis of remediation and recovery efforts	▪ Breach response can impact control documentation and risk reporting ▪ Internal auditors rely on finance to ensure cyber incidents are reflected in risk assessments	▪ Legal and investor relations rely on finance to prepare incident language for 10-Ks or 8-Ks ▪ Missed materiality or underreporting can lead to reputational damage and penalties

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Who's In the Room? Mapping the Incident Response Team

- Incident response is cross-functional; no one team owns the entire breach:
  - IT/security lead detection, containment, and technical triage
  - Legal manages regulatory exposure, discovery risk, and communications
- Finance ensures accurate financial quantification and loss disclosure:
  - Identifies insured vs. uninsured costs and tracks remediation spend
  - Coordinates with auditors and regulators on financial impact reports
- Effective IR teams include pre-identified finance representation:
  - Ideally, finance should be present during tabletop exercises and policy drafting
  - IR plans must clearly assign finance roles and responsibilities

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Finance's Role at Every Stage of an Incident

- Pre-incident: help define financial thresholds and response plans:
  - Map financial systems to risk classifications and access tiers
  - Identify potential breach disclosure triggers under SEC, GDPR, and GLBA
- During incident: track direct/indirect costs and assist with decision-making:
  - Costs may include legal counsel, third-party forensics, overtime, or reputational mitigation
  - Determine financial materiality and prepare reporting narratives
- Post-incident: lead financial remediation, reporting, and audit response:
  - Support cyber insurance claim documentation and regulatory filings
  - Update internal controls and document lessons learned

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Security Event vs. Security Incident

Security event

- Observable activity in an information system or network
- Examples:
  - 5 failed GL logins from same user
  - New vendor added within spend threshold
- Typical response: routine monitoring; log review
- Risk level: low-to-medium; monitored via KPIs

Security incident

- Confirmed violation of security policy, law, or control
- Examples:
  - Unapproved change to vendor bank account
  - Payroll file encrypted by ransomware
- Immediate escalation; treasury wire freeze; loss quantification
- Risk level: high; may trigger SOX deficiency or 8-K disclosure

SURGENT ACCOUNTING & FINANCIAL EDUCATION

What the SEC, SOX, and GLBA Expect From Finance During a Breach

- SEC Form 8-K (Item 1.05) requires disclosure of material incidents:
  - For domestic registrants, disclosure of material cybersecurity incidents must be filed on Form 8-K[1]
  - Finance must collaborate with legal to ensure accuracy and defensibility
- Internal controls over financial reporting may need to be updated if a cyber incident impacts accounting systems:
  - Breach impact on financial systems (e.g., GL, payroll) should be documented
  - Control deficiencies may need to be reported and remediated
- Gramm-Leach-Bliley (GLBA) Act and the FTC Safeguards Rule require financial institutions to maintain robust breach response plans:
  - Plan must address detection, containment, customer notification, and reporting to regulators

1. Source: U.S. Securities and Exchange Commission (SEC), *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure: A Small Entity Compliance Guide*, available at https://www.sec.gov/resources-small-businesses/small-business-compliance-guides/cybersecurity-risk-management-strategy-governance-incident-disclosure

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Critical Financial Controls That Support Incident Readiness

- Segregation of duties (SoD) helps prevent fraud during a breach:
  - Enforce dual authorization for wire transfers, account changes, or GL entries
  - Maintain system access logs and periodic access reviews
- Emergency spending protocols allow quick response:
  - Establish pre-approved vendor lists for cyber response vendors and legal counsel
  - Budgeting frameworks should support incident-driven reallocation
- Automated alerts and logging improve transparency:
  - Alerts on large transactions or failed login attempts can flag issues
  - Secure audit trails support forensic investigation and compliance audits

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Real World Case: What Happens When Finance Isn't at the Table

Case summary

Incident: In 2021, Flagstar Bank experienced a cybersecurity breach but failed to promptly assess its materiality and disclose it in a timely manner

SEC charged Flagstar for not having disclosure controls and procedures designed to ensure that relevant information about cybersecurity incidents was assessed and disclosed appropriately

Outcome: Flagstar agreed to a cease-and-desist order and paid a $3.55[1] million civil penalty without admitting or denying the SEC's findings

Key takeaway — finance must be engaged from day one

Without financial input, impact assessment is often incomplete

Cross-functional coordination must be practiced in advance

Policy recommendation: codify finance's role in IR plans

Require finance review of breach-related financial impacts before external disclosures

Ensure alignment between breach response, internal reporting, and any regulatory or audit requirements

1. Source: https://www.sec.gov/enforcement-litigation/administrative-proceedings/33-11343-s

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Bridging the Communication Gap – IT, Finance, and Legal

- Cross-functional language differences can delay response:
  - IT may talk in terms of "attack vectors" while finance needs cost mapping
  - Legal focuses on privacy law while finance focuses on materiality
- Create shared terminology and timelines in the IR plan:
  - Use visuals or templates to align stakeholders
  - Clarify when finance becomes the lead communicator
- Establish regular joint simulations and table-top exercises:
  - Include scenarios involving financial systems (e.g., payroll hack, vendor fraud)
  - Build muscle memory and relationships before a real breach

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Proactive Steps Finance Teams Can Take Today

- Review and revise your organization's IR policy with finance in mind:
  - Ensure finance is included in contact trees and breach assessment procedures
  - Add pre-approved financial templates for breach tracking and disclosures
- Develop a cyber cost tracker and impact analysis tool:
  - Capture both immediate costs and long-tail impacts (e.g., churn, lost revenue)
  - Align with internal audit and insurance documentation standards
- Join the incident response team or data governance council:
  - Bring financial acumen to cybersecurity planning
  - Advocate for risk-informed budget prioritization

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Practical Incident Response Readiness Checklist for Finance Leaders

- Have you documented a financial materiality threshold for cyber events?
- Is finance included in tabletop simulations and breach playbooks?
- Do you know how to estimate the cost of downtime, lost revenue, or legal liability?
- Do you have access to cyber insurance coverage terms and contacts?
- Have you briefed the board or audit committee on breach disclosure plans?

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Chat Prompt

Has your finance team ever participated in a cybersecurity tabletop exercise or breach simulation?

If so, what did you learn?
If not, what role do you think you'd play in a real incident?

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Analyze real-world cybersecurity incidents to identify lessons for organizational improvement

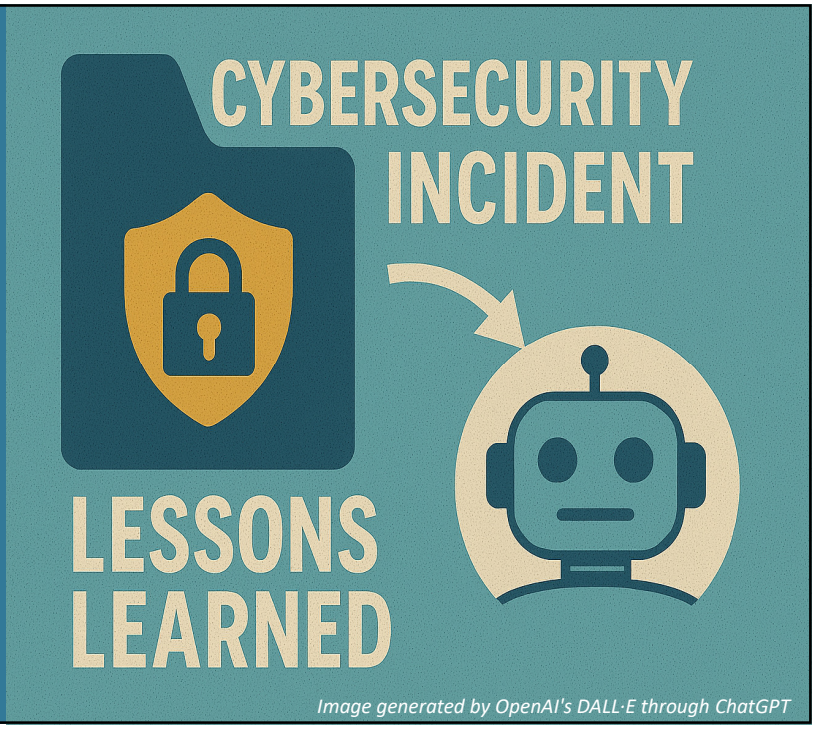


Image generated by OpenAI's DALL·E through ChatGPT

Why AI-driven Misconfigurations Are Emerging

AI projects move at high speed

- Teams quickly create new space in cloud storage and share data in hours to train new models

A single "magic link" can open the vault

- In the 2023 Microsoft case, an employee posted a download link that quietly unlocked 38 TB of internal files—passwords, Teams chats, backups[1]

Traditional security checks get skipped

- Because the work was experimental, no one ran the usual access-approval process

Standard monitoring tools don't always flag it

- Over-permissive links look legitimate to legacy data-loss systems

Why finance should care

- Leaked financial data can trigger control deficiencies and unplanned remediation costs
- Board and audit committees will ask: "How did a single link expose so much?"

1. Source: Kan, M. *"Microsoft AI Employee Accidentally Leaks 38 TB of Data."* PCMag, 18 Sep 2023. https://www.pcmag.com/news/microsoft-ai-employee-accidentally-leaks-38tb-of-data

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Case Study – Microsoft AI Data Exposure via GitHub

- What happened:
  - Microsoft AI researchers accidentally published 38TB of internal data on GitHub[1]
  - Exposed files included credentials, passwords, and employee data
- Financial and compliance consequences:
  - Potential impact on internal access controls and disclosures required under SEC rules and SOX Section 404
  - Required large-scale remediation, internal control reviews, and board briefing
- Takeaway for finance teams:
  - AI experimentation must follow IT governance and data access policies
  - Finance leaders should inquire whether R&D, analytics, or GenAI teams follow secure coding and access reviews

1. Source: Kan, M. *"Microsoft AI Employee Accidentally Leaks 38 TB of Data."* PCMag, 18 Sep 2023. https://www.pcmag.com/news/microsoft-ai-employee-accidentally-leaks-38tb-of-data

SURGENT ACCOUNTING & FINANCIAL EDUCATION

What Went Wrong in the Microsoft 38 TB Leak

Sharing AI models
- An employee posted a public download link so outside developers could get sample AI files
- Finance angle: link seemed harmless — only open-source code was expected to be shared

The hidden mistake
- The link carried a "master key" that unlocked the entire cloud vault, not just the sample files
- Finance angle: Anyone with the link could view backups, passwords, and Teams chats — potential control failure

Accidental exposure discovered
- Security firm Wiz found the link during an internet scan and quietly alerted Microsoft
- Finance angle: shows how outsiders can stumble onto mis-shared data, creating unplanned disclosure risk

Microsoft's fix
- Microsoft revoked the key within hours and started scanning for other risky links
- Finance angle: rapid response limited damage but still required board briefing and cleanup costs

Lessons for finance teams
- Don't rely on "links" alone — verify how sensitive data is fenced off
- Include cloud-storage reviews in internal-control testing
- Budget for automated scans that flag overly broad sharing keys

Source: Kan, M. *"Microsoft AI Employee Accidentally Leaks 38 TB of Data."* PCMag, 18 Sep 2023. https://www.pcmag.com/news/microsoft-ai-employee-accidentally-leaks-38tb-of-data

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Finance Quick-action Checklist

Stay protected:

Ask IT team to share cloud files through links that expire within 24 hours and allow "view-only" access

Add quarterly audit of cloud-storage permissions and token scanners (automated security scan)

Ensure finance data (GL, payroll, forecasts) lives in separate storage accounts with private endpoints

If it happens:

Freeze affected storage account, rotate keys

Engage cyber-insurance panel or legal team for forensic review and breach guidance

Assess whether incident affects financial reports, compliance filings, or vendor contracts

Update internal controls documentation to reflect added security reviews

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Emerging Threat Pattern – Shadow AI Use in Finance Departments

What's happening?

Employees are using GenAI tools like ChatGPT or Google Gemini to generate financial memos, client responses, or even budget forecasts — often without IT or compliance oversight

This unmonitored usage is referred to as "Shadow AI"

Risks for finance teams

Sensitive data (budgets, salaries, forecasts) may be pasted into AI tools, creating potential confidentiality, regulatory, or IP exposure

No audit trail or control review exists for outputs used in financial analysis or board communications

Takeaway

Establish clear GenAI use policies and require disclosure of AI-generated content in critical documents

Ensure IT is aware of all tools in use — even browser plugins or AI assistants embedded in software

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Chat Prompt

What's one GenAI tool you've seen (or used) in a finance or accounting context — and how could it potentially create a risk if used without oversight?

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Apply frameworks such as the NIST Cybersecurity Framework to practical scenarios

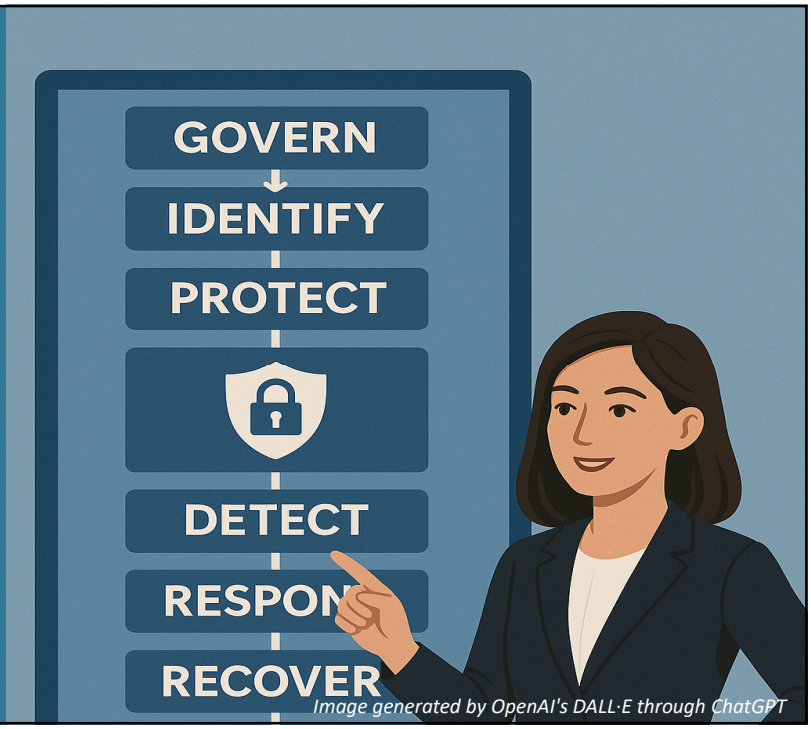


Image generated by OpenAI's DALL·E through ChatGPT

Applying the NIST Cybersecurity Framework CSF 2.0 in Finance

Why NIST CSF Matters for Finance Professionals	Integrated Approach to Risk Management	Promotes alignment between finance, IT, and legal for unified cyber governance
▪ Translates technical cybersecurity concepts into business risk language relevant to finance ▪ Helps identify gaps in internal controls tied to systems, vendors, or reporting ▪ Supports risk-based approaches that align with SOX, GLBA, and GDPR compliance efforts ▪ Framework maps to data security, incident response, and audit-readiness obligations	▪ The six core functions (Govern, Identify, Protect, Detect, Respond, Recover) offer structure for managing evolving threats ▪ Particularly valuable in a finance environment reliant on cloud-based tools and external vendors	▪ Ensures risk decisions are informed by operational, legal, and financial impacts

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Core Functions of the NIST CSF Framework 2.0

- Core functions overview:
  - The NIST CSF 2.0 is organized around six core functions that guide organizations in managing cybersecurity risk
  - These functions work together to provide a comprehensive approach to security

Govern	Identify	Protect	Detect	Respond	Recover

  - Framework is flexible — can be scaled from small firms to multinational F&A teams
  - Adopted by public companies, banks, nonprofits, and even regulatory bodies

Source: National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0; https://www.nist.gov/cyberframework*

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Govern Function – Finance Lens

Set the tone and policy direction	Define roles, responsibilities, and accountability	Resource and budget governance	Monitor performance and ensure compliance
Board/CFO approve a documented cyber-risk appetite tied to financial materiality thresholds Publish (and annually refresh) a Cyber and Gen-AI Usage Policy that covers third-party tools and disclosure timelines	Assign an accountable control owner for each finance system (GL, ERP, treasury) and any Gen-AI rules that touch financial data Embed segregation of duties and escalation paths in the policy; reference control principles	Allocate funding for controls, monitoring, and incident-response testing; track ROI (cost of control vs. potential loss) Require annual cyber-training completion rates for finance staff	Receive quarterly dashboards showing KPIs (e.g., MFA coverage, patch SLA) and KRIs (attempted BECs, near-misses) Align reporting with applicable cyber-disclosure regulations (e.g., SEC Form 8-K / 10-K) and monitor readiness for global requirements (e.g., GDPR, DORA))

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Identify Function – Finance Lens

- Understand what you need to protect:
  - Inventory high-risk systems and data (e.g., GL, payroll, treasury portals)
    - Includes shadow IT (e.g., spreadsheets with sensitive data outside secured platforms)
  - Evaluate access privileges and roles in financial systems
    - Map access against job function and segregation of duties
- Build a finance risk register:
  - Document top risks (e.g., ACH fraud, invoice manipulation, vendor impersonation)
    - Include likelihood, impact, and controls in place
  - Communicate risks to cross-functional leadership and the board
    - Supports informed budgeting and compliance decisions

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Protect Function – Finance Lens

- Limit exposure through controls:
  - Implement MFA, least privilege access, and session timeouts for financial systems:
    - Protects against phishing and credential reuse in high-value environments
- Require dual authorization for wire transfers or payment file uploads:
  - Ensures safeguards align with fraud risk and materiality
- Train and test your team:
  - Conduct phishing simulations targeting AP and payroll staff:
    - Measure results and adjust awareness campaigns
  - Include cybersecurity protocols in finance onboarding:
    - Reinforces expectations around data handling and vendor access

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Detect Function – Finance Lens

- Monitor for anomalies in financial workflows:
  - Set up alerts for after-hours logins or IP mismatches in cloud accounting software:
    - Helps catch credential theft or session hijacking
  - Detect abnormal invoice patterns, such as payment re-routing or vendor changes:
    - May signal business email compromise (BEC)
- Continuous monitoring improves audit readiness:
  - Logs must be retained and reviewable by internal audit and compliance teams:
    - Demonstrates control effectiveness over time
  - Leverage SOC 2/Type II data from finance-related vendors:
    - Confirms third-party systems meet your monitoring standards

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Respond Function – Finance Lens

- Finance-led incident planning:
  - Pre-define roles for CFO, controller, and treasury during a cyber event:
    - Who stops payments, communicates with banks, evaluates materiality?
  - Map potential financial reporting impact:
    - Delays in closing books, loss events requiring disclosure, insurance considerations
- Coordinate internally and externally:
  - Practice tabletop scenarios involving wire fraud or vendor compromise:
    - Include finance, legal, IT, comms, and audit
- Prepare breach notification templates for clients and regulators:
  - Align with GDPR, SEC 8-K, and GLBA requirements

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Recover Function – Finance Lens

- Finance resilience planning:
  - Establish recovery time objectives (RTO) for payroll, AP, and ERP access:
    - What's the acceptable downtime before financial or reputational harm?
  - Maintain offline backups of critical accounting data and reports:
    - Especially important for year-end reporting, audit support, or payroll
- Strengthen controls based on lessons learned:
  - Perform post-mortem analysis on failed or bypassed controls:
    - Update policies, training, and control documentation
  - Use findings to justify future cybersecurity investments:
    - e.g., stronger vendor vetting, software upgrades, or insurance policy review

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Hypothetical Wire Transfer Fraud Scenario

- Context: Business Email Compromise (BEC) *(illustrative case)*
  - Attacker impersonates CFO and requests urgent wire to fraudulent vendor account
  - Accounts payable staff bypasses second approver due to social engineering
  - Impact if undetected: A high-value, unauthorized wire—often reaching six figures—can drain working capital and disrupt payroll or vendor payments
  - Why this matters to small and medium-sized businesses: banks may shift the loss to the company under UCC Article 4A if agreed security procedures were followed; cyber-insurance deductibles and lender covenants can add further financial strain
  - Why this matters to CPAs: auditors view control overrides — like bypassing payment approvals — as serious red flags that may require documentation, remediation, or disclosure depending on the risk

SURGENT ACCOUNTING & FINANCIAL EDUCATION

NIST CSF 2.0 Controls for BEC Wire Fraud (Illustrative)

CSF 2.0 function	Existing control gaps	Actionable steps for accounting/treasury teams
Govern	No board-approved wire transfer policy or risk appetite statement	• Add *executive-impersonation* to the cyber risk appetite statement • Require written policy that any wire > $ X **must** be confirmed on a second channel
Identify	Finance risk register omits "executive impersonation"	• Flag "new vendor + high-value transfer" as a *critical asset* in the risk register • Map who can create or edit vendor bank details; review SoD quarterly
Protect	MFA not enabled for email; no out-of-band payment verification	• Enforce MFA on CFO/AP mailboxes • Build an ERP control that blocks same-day wires unless dual approval + callback field completed
Detect	No alerts for new vendor bank changes or unusual IP logins	• Configure SIEM/SOC rule: alert on "new vendor + first payment > $25 k" • Use mailbox-rule monitoring to catch auto-forward tricks
Respond	Treasury unsure who to notify or how to freeze funds	• Add a **"pause-and-verify"** step to the IR playbook: treasury contacts bank, issues recall/hold harmless within minutes • Pre-draft an 8-K template for material fraud
Recover	No incident log or post-incident control review occurred	• Log incident in controls deficiency tracker; update training slides • Conduct a lessons-learned session; tighten thresholds or add voice biometrics

SURGENT ACCOUNTING & FINANCIAL EDUCATION

BEC Quick Action Checklist (Based on FBI IC3 Guidance)

Stay protected:

Verify any account change or wire request on a second channel (phone, secure chat)

Check sender address carefully—mobile mail apps often truncate domains

Enable full email-header view in Outlook/Gmail for staff who approve payments

Review banking transactions daily; set text alerts for wires > $ X

If it happens:

Call your bank immediately – request a recall/reversal and provide a hold harmless letter

File an IC3 complaint at www.ic3.gov with full wire details (routing, SWIFT, intermediary bank)

Activate the incident-response playbook: freeze further wires, notify CFO/legal/insurer, estimate loss

Update your risk register and training based on lessons learned

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Hypothetical Ransomware Disruption

- Context: Payroll Platform Compromised (illustrative case)
- Ransomware attack disables hosted payroll provider; employees go unpaid for 5 days
- Framework breakdown:
  - Govern: no board-level policy requiring payroll vendors to meet defined RTO/RPO targets
  - Identify: risk not previously documented in vendor risk register
  - Protect: vendor's backup and recovery protocols not verified during onboarding
  - Detect: finance team notices issue only after failed payroll processing
  - Respond: no contingency plan for alternate payroll processing or notification
  - Recover: poor vendor transparency slowed communication and damage control

SURGENT ACCOUNTING & FINANCIAL EDUCATION

NIST CSF 2.0 Controls for Payroll Ransomware (Illustrative)

CSF 2.0 function	Existing control gaps	Actionable steps for accounting/treasury teams
Govern	No board-level policy requiring payroll vendors to meet specific RTO/RPO targets	• Embed **≤ 24 h RTO / ≤ 4 h RPO** in vendor contracts • Require annual attestation of ransomware resilience
Identify	Payroll outage risk not previously documented in vendor risk register	• Classify payroll as *mission-critical*; rate vendor outage impact and likelihood • Track single-vendor concentration risk
Protect	Vendor's backup and recovery protocols never verified during onboarding	• Request SOC 2 (Type II) or ISO 22301 report • Include right-to-audit for off-site encrypted backups
Detect	Finance learns of issue only after failed pay run	• Add vendor "heartbeat" alerts in ERP (API-status ping) • Subscribe to vendor status-page SMS notifications
Respond	No tested contingency for alternate payroll processing or employee notice	• Pre-contract secondary payroll bureau; maintain import template • Draft employee comms scripts; keep contacts offline
Recover	Poor vendor transparency slowed status updates and damage control	• Hold post-incident review with vendor; add penalty clause for future SLA breaches • Update business-impact analysis with real outage costs

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Ransomware Quick Action Checklist (Based on CISA/NIST Guidance)

Stay protected:

Vet vendors before signing — require proof of immutable, offline backups and an annual restore test

Keep off-line copies of the latest payroll export and pay-rules

Enforce MFA and segregated admin credentials for vendor portals

Subscribe to vendor status page SMS/email alerts for service degradation

Test the payroll outage playbook annually and record outcomes

If it happens:

Activate the alternate payroll channel or issue emergency manual checks

Notify employees immediately with payment ETA and FAQs

Contact your cyber-insurance carrier and engage forensic support if covered

Request a detailed timeline and status updates from the vendor (e.g., every 4 hours)

Log all costs and lessons learned; update the vendor contract and risk register accordingly

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Deep Fake Voice Fraud: $35 Million Heist in the U.A.E.

- Incident Summary:
  - Target: a bank in the United Arab Emirates (UAE)
  - Method: fraudsters trained a neural text-to-speech model on the director's public recordings, producing a real-time voice clone
  - Deception: the clone called a bank manager, and convincingly instructed the manager to transfer $35 million to various accounts
  - Outcome: the bank manager, believing they were speaking to the authorized director, processed the fraudulent transactions
  - Key takeaway: generative AI tools can bypass traditional voice verification methods and highlight the increasing sophistication of social engineering attacks, raising the bar for payment controls

Source: Brewster, Thomas in Forbes, "Huge Bank Fraud Uses Deep-Fake Voice Tech To Steal Millions," published October 14, 2021, https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Deep Fake Voice Fraud – What Finance Teams Should Do Next

Tighten payment verification	Always confirm high-value transfer requests on a second channel – e.g., call a known number, use secure chat, or require a dual-approval click in the ERP Never act on voice instructions alone
Add a "pause-and-alert" step to the playbook	If a call feels rushed or unusual, pause the payment, save the recording, and notify Treasury + Security right away
Teach staff the red flags	Refusal to switch channels ("I'm boarding a plane, just do it now…") Urgent, high-dollar requests outside normal workflow
Plan for better tools	Work with IT to evaluate voice-biometric or deep-fake-detection services; include the cost in next year's budget
Close the loop	Document any loss, update internal control documentation, and consult legal or compliance teams on whether external disclosure (e.g., to regulators or investors) is required

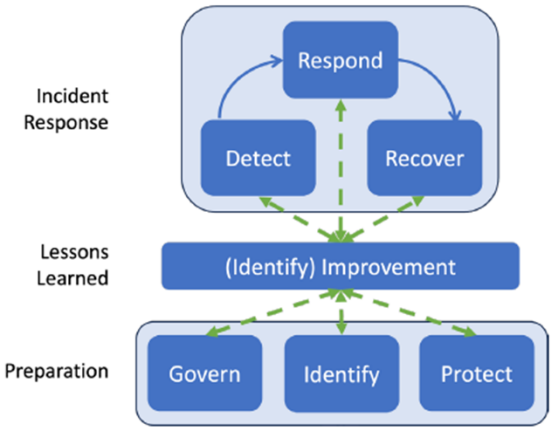
SURGENT ACCOUNTING & FINANCIAL EDUCATION

Mapping COSO to NIST in Finance Teams

- Why COSO and NIST work together:
  - COSO addresses internal controls over financial reporting (ICFR)
  - NIST provides a cybersecurity-specific lens on control structure and effectiveness
- Examples of alignment:
  - COSO Control Environment ↔ NIST Identify: tone at the top, system risk awareness
  - COSO Risk Assessment ↔ NIST Detect/Protect: ongoing identification of fraud/cyber threats
  - COSO Monitoring Activities ↔ NIST Recover: post-incident reviews and process enhancement

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Incident Response Life Cycle Model Based on NIST CSF 2.0 Functions



Source: Nelson A, Rekhi S, Souppaya M, Scarfone K (2025). *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.* NIST Special Publication 800-61r3. https://doi.org/10.6028/NIST.SP.800-61r3
Republished courtesy of the National Institute of Standards and Technology.

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Key Communication Channels During Incident Response

Law enforcement and regulators	FBI, SEC, or state agencies may require notification. Critical for legal protection and compliance.
Vendors and service providers	SaaS tools (e.g., payroll, GL platforms) must be notified if they are impacted. May help contain damage or restore services.
Cyber insurance and legal counsel	Public disclosure may be needed depending on the breach scope. Communications must be accurate, timely, and coordinated with legal.
Customers, constituents, and media	Public disclosure may be needed depending on the breach scope. Communications must be accurate, timely, and coordinated with legal.

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Chat Prompt

After a breach, your organization files a cyber insurance claim. The insurer requests detailed documentation of system downtime, lost revenue, and legal costs.

Is your finance team prepared to provide this information? What would you need?

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Collaborate effectively with IT and legal teams during cybersecurity crises

Image generated by OpenAI's DALL·E through ChatGPT

Why Collaboration Matters During Cyber Incidents

- Cyber incidents cross silos:
  - Security breaches impact IT systems, financial operations, legal risk, and external reputation
  - Effective response depends on timely, aligned decisions across departments
- Finance is essential to crisis response:
  - Finance may detect anomalies (e.g., unauthorized wire transfers, suspicious spending)
  - Plays a key role in cost estimation, disclosure materiality, and insurance claims
- Legal ensures compliance and containment:
  - Disclosure obligations — such as breach notification laws or contract requirements — often require legal interpretation
  - Legal supports evidence preservation and privilege protection

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Common Collaboration Challenges

- Siloed communication and delays:
  - Lack of shared protocols can lead to duplicate or conflicting actions
  - Time-sensitive regulatory notifications may be missed
- Unclear roles or handoffs:
  - Who leads incident classification, disclosure decision-making, and regulator communication?
  - Misalignment delays containment or triggers audit issues
- Overload and panic during crises:
  - Information overload and unclear command structures can paralyze response teams
  - Emphasizes need for pre-defined playbooks and tabletop rehearsals

SURGENT ACCOUNTING & FINANCIAL EDUCATION

What Effective Collaboration Looks Like

- Defined roles and escalation paths:
  - Use of RACI matrix (responsible, accountable, consulted, informed) across legal, finance, and IT
  - Pre-assigned leads for response, disclosure, and recovery planning
- Regular joint training and simulations:
  - Finance staff join incident response drills (e.g., ransomware tabletop)
  - Legal helps review response templates and privilege strategies
- Integrated communication plans:
  - Shared internal reporting platform or war room structure
  - Legal reviews customer/regulator communication before release

SURGENT ACCOUNTING & FINANCIAL EDUCATION

When Accounting and Finance Should Engage Legal

- Material breach determination:
  - Legal helps interpret thresholds for disclosure or notification requirements (e.g., regulators, GDPR, or contracts)
  - Finance provides loss estimates and operational disruption impact
- Litigation and insurance considerations:
  - Certain breaches trigger lawsuits or insurance claims
  - Legal and finance collaborate on documentation, evidence preservation, and cost tracking
- Privilege and confidentiality protection:
  - Legal may advise limiting written communications or routing info through counsel
  - Accounting and finance must be trained on when/how to communicate during active investigations

SURGENT ACCOUNTING & FINANCIAL EDUCATION

When Finance Must Engage IT

- Investigating root causes and scope:
  - Finance may help trace unauthorized transactions, payment system manipulation, or file access logs
  - IT provides forensics support and logs to help attribute loss sources
- Restoring financial systems:
  - If ERP or payroll systems are disrupted, finance must coordinate data validation and restoration with IT
  - Clear protocols needed for restoring backups and confirming integrity
- Cost tracking for remediation and reporting:
  - IT logs recovery costs (e.g., consultants, software upgrades) and shares with finance
  - Finance maps costs to accounts for internal reporting and disclosures

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Coordinated Cyber Incident Response Workflow (Aligned with NIST CSF 2.0)

1. Govern (Pre-Incident)
- Roles and responsibilities defined (e.g., finance, IT, legal, HR)
- Incident response plan tested through tabletop exercises
- Tools and vendor contacts are updated and accessible

2. Identify
- Critical payroll and GL assets inventoried
- Vendor risk scores documented
- Seg of duties map maintained

3. Protect
- MFA on CFO/AP e-mail and ERP
- Immutable backups and DR drills
- Staff phishing simulations

4. Detect
- SIEM alert: “new vendor + first payment > $25 k”
- Vendor status-page monitoring
- UEBA for off-hours logins

5. Respond
- Incident Response Team (IRT) activated
- Communication protocols followed (internal + external)
- Containment and mitigation actions executed

6. Recover
- Impacted systems restored, payroll or financial workflows validated
- Confirm that data integrity and availability are restored
- Stakeholder communications coordinated with legal/compliance

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Summary – Key Takeaways for Finance Teams

- Build relationships before a crisis:
  - Know who your IT and legal contacts are, and what they handle during an incident
- Join cross-functional response planning:
  - Finance is not just a support role — it's part of the core team
  - Be ready to lead loss quantification and disclosure inputs
- Understand where finance fits in frameworks:
  - Familiarize yourself with NIST, COSO, and incident response playbooks to avoid confusion during real events

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Chat Prompt

Think of a time when collaboration across departments worked well — or didn't.

What do you think are the most important factors for smooth collaboration between finance, IT, and legal during a crisis?
Can you name one thing finance should do before an incident to build that trust?

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Develop strategies for integrating incident response lessons into proactive risk management

Image generated by OpenAI's DALL·E through ChatGPT

Introduction – Why Lessons Learned Matter

- Incident response is not complete until lessons are analyzed and acted upon:
  - Post-incident learning reduces recurrence
  - Supports stronger control environments
- Financial professionals can use findings to improve risk assessments:
  - Update risk tolerance thresholds and controls based on actual impact
  - Inform board-level reporting and risk disclosures

SURGENT ACCOUNTING & FINANCIAL EDUCATION

What Happens After "Lessons Learned"?

Many organizations stop at the postmortem—no follow-through

Lessons are documented but not prioritized

Control owners may not be informed or accountable

Finance's role: ensuring that response outcomes are budgeted, reported, and integrated

Risk mitigation plans must tie back to lessons learned

If it affected financial systems, it should update control assessments

From Response to Risk Register – Practical Steps

Every breach should prompt a review of

- Risk register entries (do they reflect actual threat levels?)
- Internal controls tied to the breach (were they adequate?)

Lessons should feed into

- Updated control testing scopes
- Budget reallocation (e.g., endpoint detection, training)

Integrating Lessons into the Risk Management Framework Cycle

- Continuous improvement:
  - Post-incident analyses should feed into the RMF's core functions: frame, assess, respond, and monitor
- Risk reassessment:
  - Use incident findings to reassess risk tolerance and update the risk register accordingly
- Control enhancements:
  - Implement new or improved controls based on identified vulnerabilities
- Monitoring adjustments:
  - Adjust monitoring strategies to detect similar threats proactively

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Accounting and Finance's Role in Post-incident Risk Management

Risk tolerance review:	Assess whether the incident indicates a need to adjust the organization's risk appetite
Control tailoring:	Customize financial controls to address specific vulnerabilities revealed by the incident
Ongoing monitoring:	Implement continuous monitoring of financial systems to detect anomalies indicative of similar threats

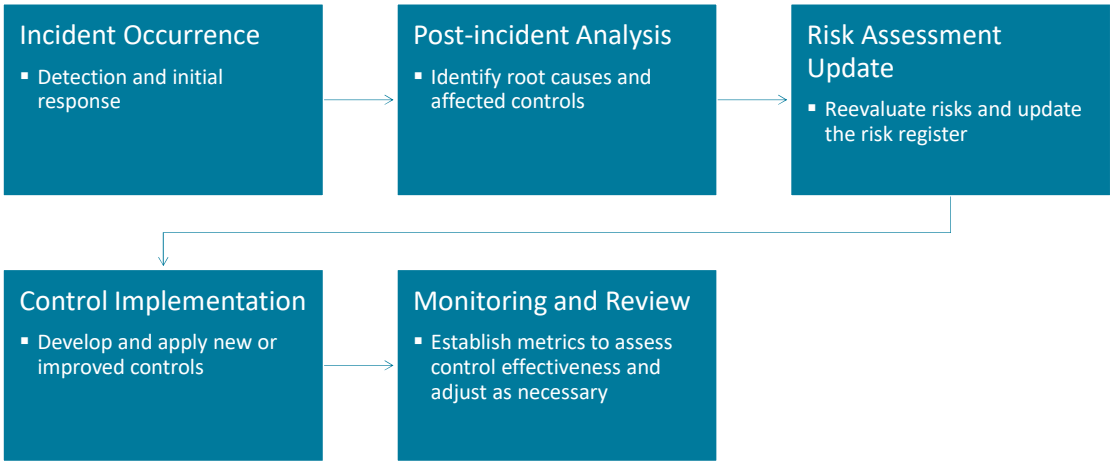
SURGENT ACCOUNTING & FINANCIAL EDUCATION

Communicating Post-incident Improvements

- Regulatory reporting:
  - Ensure compliance with applicable reporting requirements — whether to regulators, insurers, or legal counsel
- Board updates:
  - Provide the board with insights into incident impacts and the steps taken to mitigate future risks
- Audit trail:
  - Maintain comprehensive documentation of the incident response and subsequent control enhancements for audit purposes

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Workflow: From Incident to Strategic Risk Management



SURGENT ACCOUNTING & FINANCIAL EDUCATION

Chat Prompt

Think about a security incident, audit finding, or IT control failure you've encountered — big or small

What changed afterward?
Was there a new control, policy, or risk register update?

Chat Prompt

A finance team member receives an email that looks like it's from your payroll provider. It asks them to "confirm account credentials to avoid service interruption." They click the link and enter their login. Within hours, bank routing details for several employees are changed.

What should happen next?
Does your team have a plan to respond to this kind of incident?
Who would you notify first?

Reflection Activity

Final Reflection – What Will You Take Forward?

If a cybersecurity incident were to occur in your organization tomorrow…

- Do you think you or your finance team would be included in the post-incident review?
- If yes, how could you contribute?
- If not, what could you do to ensure your voice is part of the conversation?

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Cybersecurity Risk Management for Financial Professionals: Policies, Controls, and Emerging Threats

CYR2/25/W1

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

1

"Technology trust is a good thing, but control is a better one."

—Stephane Nappo, Global Cybersecurity Leader

Source: Nappo, S. (n.d.). *Quotes*. Goodreads. Retrieved from https://www.goodreads.com/author/quotes/19698507.Stephane_Nappo

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

2

Learning Objectives

- Identify essential components of a cybersecurity risk management program, including policies and controls
- Evaluate cybersecurity risks, and develop risk mitigation strategies tailored for financial professionals
- Understand global compliance standards, such as the EU AI Act and GDPR, and their implications for U.S.-based organizations
- Analyze financial impacts from cybersecurity breaches using real-world case studies
- Apply cybersecurity policies and controls that align with U.S. regulatory frameworks while addressing global compliance trends

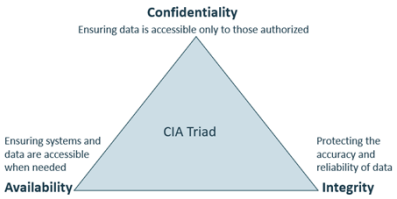
SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Identify essential components of a cybersecurity risk management program, including policies and controls

Image generated by OpenAI's DALL·E through ChatGPT

What Is Cybersecurity Risk Management?

- Protects systems, data, and operations from evolving threats:
  - Includes both technical vulnerabilities and human errors
  - Focuses on confidentiality, integrity, and availability (CIA)
- Applies risk principles to cyber threats:
  - Identify, assess, and respond to cybersecurity risks
  - Prioritize based on likelihood and business impact
- Foundation for compliance and trust:
  - Supports SOX, GDPR, and internal audit standards
  - Builds confidence with customers, partners, and regulators



SURGENT ACCOUNTING & FINANCIAL EDUCATION

Why It Matters for Finance Professionals

- Finance teams manage high-value targets:
  - Payments, payroll, and vendor data are prime for exploitation
  - AI-powered fraud can mimic authority and bypass controls
- Cyber risk is now financial risk:
  - Incidents trigger financial reporting obligations
  - Breaches can impact valuation and investor confidence, and expose control weaknesses that may require remediation and documentation
- Financial professionals are now cyber risk stakeholders:
  - Increasing regulatory and audit scrutiny
  - Need to assess exposure across internal control frameworks

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Core Components of a Cyber Risk Management Program

- Governance and policies:
  - Define roles, responsibilities, and escalation protocols
  - Align with standards like COSO-ERM or NIST CSF 2.0
- Risk identification and assessment:
  - Catalog systems, data flows, and known vulnerabilities
  - Evaluate risk likelihood and business impact
- Controls and monitoring:
  - Implement access controls, alerts, and testing routines
  - Monitor anomalies in behavior, timing, or approval patterns

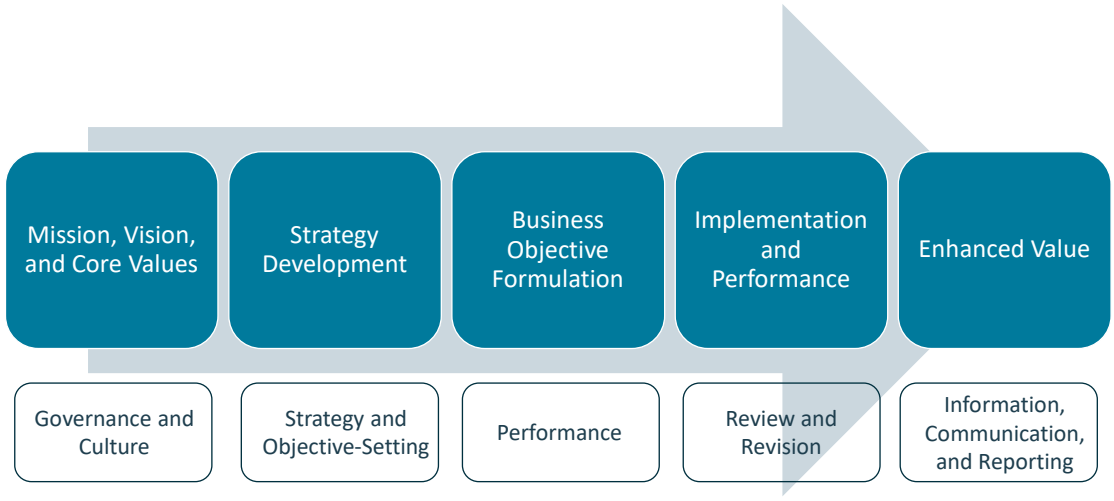
SURGENT ACCOUNTING & FINANCIAL EDUCATION

Cyber Risk Governance – Roles and Responsibilities

- Finance and audit professionals:
  - Identify high-risk processes and sensitive data
  - Evaluate control gaps in payment approvals, reconciliations
- IT and security teams:
  - Configure technical safeguards and intrusion detection
  - Share alerts and incident data with risk owners
- Executive oversight and cross-functional accountability:
  - Board, CFO, and internal audit must align on risk priorities
  - Encourage shared ownership of genAI and cyber risk governance

SURGENT ACCOUNTING & FINANCIAL EDUCATION

COSO ERM Framework



Adapted from Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management Framework, 2017

SURGENT ACCOUNTING & FINANCIAL EDUCATION

COSO and Cybersecurity Governance for Finance

- COSO ERM helps embed cybersecurity into enterprise risk strategy:
  - Encourages alignment of cybersecurity with organizational objectives
  - Promotes accountability and shared risk ownership
- Applies directly to risk oversight, internal controls, and reporting accuracy:
  - Supports risk assessment, control activities, and monitoring principles
  - Provides structure for board and audit committee oversight
- Accounting and finance leaders can use COSO to elevate cyber risk visibility:
  - Helps evaluate whether cyber threats are included in financial risk profiles
  - Enhances internal control narratives under SOX and ICFR

SURGENT ACCOUNTING & FINANCIAL EDUCATION

NIST CSF 2.0 – Finance Governance Snapshot

- NIST overview: National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 — six functions offer a common language to set, measure, and report cyber risk

Function	Finance-specific focus
Govern	Board/CFO approve cyber-risk appetite tied to SOX 404 materiality; budget for controls
Identify	Inventory critical ledgers, payroll feeds, vendor APIs; classify data sensitivity
Protect	Enforce MFA and segregation of duties on wire approvals; encrypt backup files
Detect	Use UEBA/SIEM rules to flag off-hours GL edits and new vendor bank details
Respond	Incident playbook quantifies loss for 8-K disclosure; treasury freeze-wire procedure
Recover	Test RTO ≤ 24 h for payroll; feed lessons learned into next year's budget cycle

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Lines of Defense in Cybersecurity Governance

- Three Lines of Defense model defines roles across risk functions:
  - 1st line: business units own and manage controls
  - 2nd line: risk and compliance functions guide and monitor
  - 3rd line: internal audit independently evaluates controls and risk governance
    - Verifies control design and operating effectiveness
    - Helps identify blind spots and emerging risks
- Internal audit provides independent oversight and assurance:
  - Verifies control design and operating effectiveness
  - Helps identify blind spots and emerging risks
- Accounting and finance may play multiple roles depending on function:
  - Owns financial systems (1st line) and supports testing (2nd line)
  - Partners with audit (3rd line) during SOX and ICFR reviews

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Cybersecurity Governance Priorities for Finance

- Access governance is a top priority for financial systems:
  - Define who can access, change, or approve data in GL, AP, payroll
  - Review access logs and user role assignments regularly
- Watch for shadow IT tools and unapproved AI applications:
  - Identify unsanctioned spreadsheets, SaaS apps, or AI tools
  - Vet genAI-generated financial content for control gaps
- Finance must help define cyber risk governance checkpoints:
  - Participate in vendor reviews, API access decisions, and SaaS onboarding
  - Set standards for approval, documentation, and monitoring

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Types of IT Controls in Financial Systems

- General IT controls (GITCs) protect system infrastructure and access:
  - Access provisioning, change management, and backups
  - Support reliability of systems used in financial reporting
- Application controls enforce process-level integrity:
  - Input validation, approval workflows, audit logging
  - Embedded in systems like ERP, payroll, and AP tools
- Both control types are essential for financial integrity:
  - Support accuracy, completeness, and auditability of data
  - Require regular testing and collaboration with IT teams

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Control Lifecycle – From Design to Monitoring

- Control design aligns with risk assessment findings:
  - Identify what could go wrong in finance workflows
  - Ensure controls address root causes, not just symptoms
- Implementation must match the documented policy:
  - Controls must be built correctly into systems or processes
  - Avoid “check-the-box” controls that do not actually reduce risk
- Ongoing monitoring and testing validate effectiveness:
  - Include periodic user access reviews and exception reporting
  - Document evidence for audits and compliance reviews

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Common Cyber Control Gaps in Accounting and Finance

- Shared credentials or inactive accounts:
  - Increases risk of unauthorized transactions or audit trail gaps
  - Often missed during control testing
- Lack of segregation of duties in small teams:
  - One user can initiate and approve sensitive transactions
  - Finance leaders must help identify compensating controls
- No validation of AI-generated reports or narratives:
  - Outputs may be fabricated, incomplete, or misused
  - Requires human review and clear audit documentation

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Finance and Cyber Governance – What Is Changing?

- Cyber now intersects with financial compliance:
  - SEC and PCAOB emphasize cybersecurity disclosure and oversight
  - Auditors ask how cyber risks impact ICFR
- Finance is expected to collaborate with IT and risk:
  - Cross-functional ownership of data, workflows, and controls
  - Risk registers should include cyber risks tied to finance
- Boards want visibility into cyber risk exposure:
  - CFOs increasingly report cyber impacts in risk committees
  - Cyber strategy now affects budget, audit, and compliance planning

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Chat Prompt

What is one area in your finance environment — a process, system, or report — that you believe could present a cyber-related risk if controls were weak or missing?

Think about:
Who has access?
How is activity reviewed?
What happens if the system is unavailable?

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Evaluate cybersecurity risks and develop risk mitigation strategies tailored for financial professionals

Image generated by OpenAI's DALL·E through ChatGPT

19

From Awareness to Action – Why Risk Evaluation Belongs in Accounting and Finance

- We've already seen why cyber risk matters — now let's talk about your role in evaluating it:
  - Finance owns processes tied to reporting, controls, and risk disclosure
  - Evaluation helps link cybersecurity threats to operational and financial exposure
- Risk evaluation supports internal audit, controls, and accountability:
  - Proactive risk assessment helps surface weak points before they lead to control failures
  - Internal auditors and stakeholders increasingly expect cyber risks to be addressed in finance-related risk assessments
- This module focuses on the 'how' of cyber risk management:
  - Risk identification, scoring, documentation, and mitigation workflows

SURGENT ACCOUNTING & FINANCIAL EDUCATION

20

Types of Cybersecurity Risks Relevant to Finance

System and data breaches

Unauthorized access to sensitive financial records, payroll, or vendor data

May trigger disclosure obligations under regulations or data privacy laws

Ransomware attacks

Encrypted access to critical systems like AP, GL, or reporting platforms

Operational disruption may delay filings or lead to material financial loss

Insider threats

Risk of fraud or sabotage by users with privileged access (e.g., controllers)

Also includes unintentional exposure due to weak access controls

AI-powered social engineering

Tools like deepfake audio or genAI-generated phishing increase fraud risk

Attacks often impersonate executives or manipulate financial workflows

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Risk Registers – Connecting Cyber Threats to Business Impact

- Tracks risks in a structured format:
  - Each entry includes risk name, description, likelihood, and impact rating
  - Helps align IT, finance, and audit teams on shared risk visibility
- Maps financial exposure across business functions:
  - Links each cyber threat to potential financial implications (e.g., vendor fraud → cash loss)
  - Supports enterprise risk management (ERM) and internal control narratives
- Supports governance, audit, and compliance:
  - Documents ownership, mitigation actions, and monitoring frequency
  - Demonstrates proactive oversight for SOX, ISO, or PCAOB expectations

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Qualitative vs. Quantitative Risk Assessment Approaches

- Qualitative risk assessment:
  - Uses descriptive scales (e.g., low, medium, high) for impact and likelihood
  - Best for organizations without detailed data or for early-stage risk tracking
- Quantitative risk assessment:
  - Assigns dollar-value estimates to potential losses or risk exposure
  - Supports financial modeling, scenario planning, and insurance analysis
- Choose based on context and resources:
  - Many organizations use a hybrid model: qualitative for general tracking, quantitative for high-priority risks
  - Accounting and finance teams can help translate operational risks into financial terms

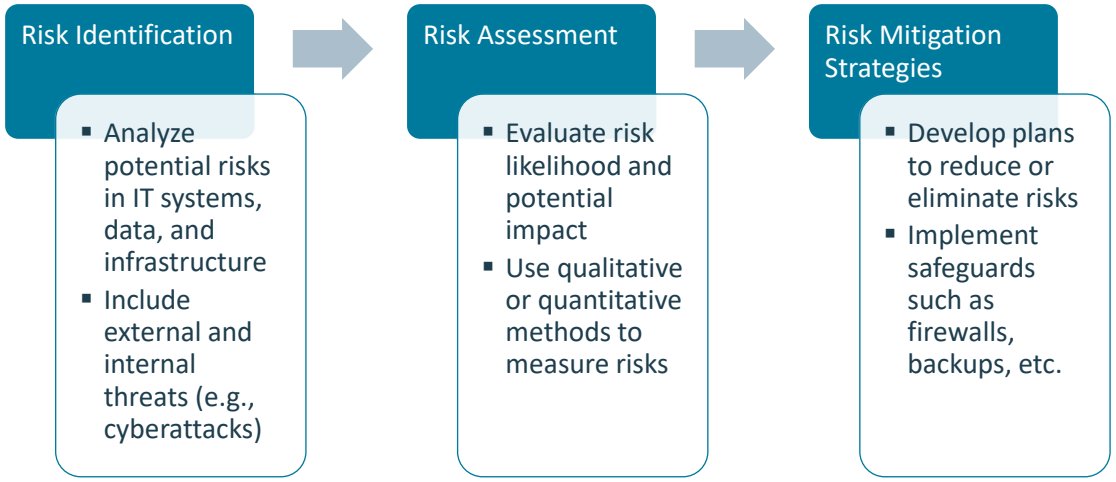
SURGENT ACCOUNTING & FINANCIAL EDUCATION

IT Risk Identification and Assessment Overview

- Identify key IT-related risks in financial systems:
  - Includes threats like data breaches, unauthorized access, and fraud
  - Focus on finance-facing systems (GL, AP, payroll, reporting tools)
- Assess impact on confidentiality, integrity, and availability:
  - Could financial data be exposed, altered, or delayed?
  - Link each IT risk to a financial or compliance consequence
- Prioritize based on risk likelihood and exposure:
  - Align with audit, SOX, and ICFR requirements
  - Use heat maps or risk matrices for visual communication

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Process of Managing and Evaluating IT Risks



Cyber Risk Appetite and Tolerance in Finance Functions

- Establishes acceptable level of cyber risk exposure:
  - Defines how much disruption or data loss is tolerable to operations
  - Finance helps frame acceptable risk in terms of dollar impact
- Informs investment in controls and resources:
  - High-risk tolerance may mean fewer controls, but higher exposure
  - Low-risk tolerance may require stronger policies, audits, and tools
- Requires board and leadership alignment:
  - Tone at the top sets culture for risk accountability
  - CFOs and controllers play a key role in translating risk to finance terms

Choosing and Documenting Cyber Risk Response Matrix

	Residual Impact - High	Residual Impact - Low
Likelihood - High	**Avoid** ▪ Block high-risk payment channel ▪ Decommission unsupported legacy app	**Mitigate** ▪ Apply MFA and segregation of duties ▪ Patch SLA ≤ 7 days
Likelihood - Low	**Transfer** ▪ Cyber-insurance rider ▪ Outsource SaaS with SLA and penalty	**Accept** ▪ Document rationale in risk register ▪ Monitor KPI quarterly

Document every decision: clearly name the control owner, record the scheduled review date, and reference the supporting evidence (policy link, SOC report, insurance certificate, etc.)

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Role of Financial Professionals in Cyber Risk Response

- Assess financial impact of a cyber event:
  - Quantify loss exposure and support materiality decisions
  - Inform cyber insurance claims and regulatory disclosures
- Support documentation for audits and control testing:
  - Track control failures, recovery actions, and remediation timelines
  - Maintain journal entries and system logs tied to financial systems
- Collaborate with IT and legal during incident response:
  - Provide financial system access or workflow context
  - Help evaluate whether internal controls were breached

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Internal Controls for Cyber Risk Mitigation

Preventive controls

Limit access to financial systems, apply MFA, automate approval rules

Reduce likelihood of fraud or errors in AP, GL, or payroll

Detective controls

Monitor for anomalies in transaction logs, GL edits, or journal approvals

Use UEBA or audit trail reviews to catch suspicious activity

Corrective controls

Establish system recovery, data restoration, and incident response protocols

Ensure business continuity for financial operations

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Chat Prompt

If a cybersecurity breach affected your finance function, who would be the first person your team would call — and what would you need to explain to them?

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Understand global compliance standards, such as the EU AI Act and GDPR, and their implications for U.S.-based organizations

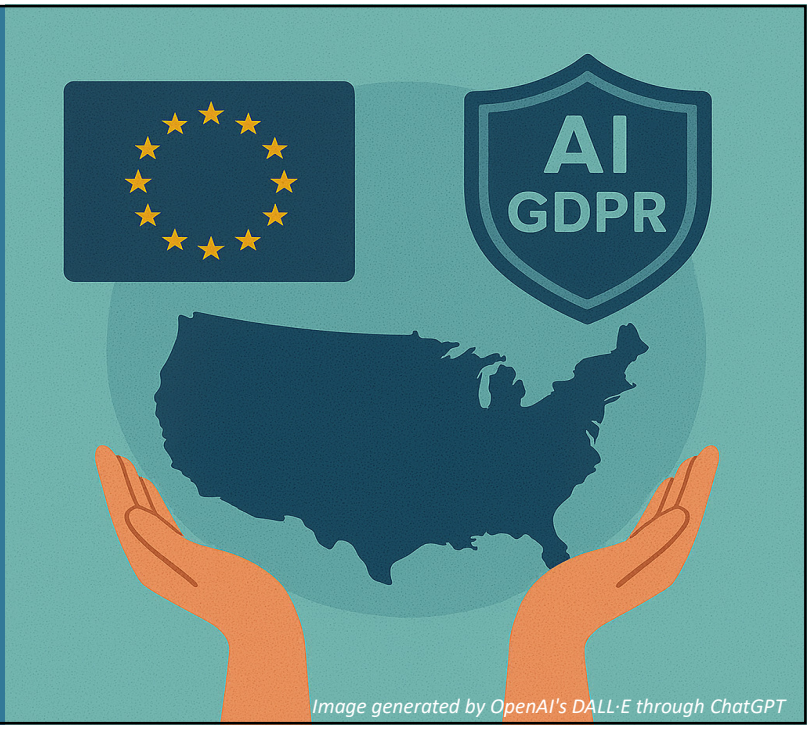


Image generated by OpenAI's DALL·E through ChatGPT

Why U.S. Finance Professionals Need To Pay Attention to Global Cyber Rules

Global regulations are increasingly affecting U.S.-based organizations	Cross-border data storage and cloud platforms often involve processing EU citizen data Noncompliance can result in fines, restrictions, or reputational damage — even for U.S.-only entities
AI and data privacy rules are now finance concerns	Finance teams rely on AI-powered tools for reporting, expense workflows, and fraud detection These systems may trigger classification or transparency requirements under global laws
Understanding the EU AI Act and GDPR prepares you for global accountability	Enables finance teams to assess AI-related risk across internal controls and compliance frameworks Helps organizations demonstrate due diligence in regulatory audits and risk disclosures

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Introduction to the EU AI Act

- Purpose of the EU AI Act:
  - Establishes a legal framework for trustworthy and ethical AI in the EU
  - Aims to protect individuals' fundamental rights while fostering innovation
- Global influence:
  - Expected to set a global benchmark for AI governance
  - Encourages safety, transparency, and accountability in AI systems
- Connection to business priorities:
  - Aligns with global values like ethical AI use and transparency
  - Supports innovation while building trust in AI technologies

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Key Definitions: AI Systems and Risk

- AI Systems (Article 3(1) of the EU AI Act):
  - Machine-based systems designed to operate with varying levels of autonomy
  - Use inputs to generate outputs such as predictions, content, recommendations, or decisions
  - Outputs can influence physical or virtual environments
- Risk (Article 3(2) of the EU AI Act):
  - Combination of the likelihood of harm occurring and the severity of that harm
  - Harm can affect individuals (e.g., discrimination), organizations (e.g., reputational damage), or society (e.g., spread of misinformation)

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Scope of the EU AI Act

Applicability: the Act applies to AI systems offered, sold, or used in the EU, including those provided by non-EU entities

Providers

Individuals, organizations, or public bodies that develop AI systems or general-purpose AI models (applies to both free and paid systems offered in the EU market)

Product Manufacturers

Entities that produce physical or digital products incorporating AI systems

Deployers

Any entity or individual (other than for personal use) that uses an AI system - most organizations subject to the EU AI Act will fall into this category

Importers

An individual or organization based in the EU that introduces AI systems from non-EU providers to the EU market

Distributors

Entities in the supply chain, other than providers or importers, that make AI systems available in the EU market

Exemptions: military applications and national security uses are excluded from the Act's purview

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Cybersecurity Obligations Under the EU AI Act

Cybersecurity is a core component of AI system compliance	Article 15 outlines specific cybersecurity expectations	Why this matters for finance professionals
▪ Applies especially to high-risk systems used in finance, HR, biometrics, and infrastructure ▪ Builds on cybersecurity principles like integrity, availability, and resilience	▪ Requires protection against adversarial attacks, tampering, and misuse ▪ Systems must include safeguards to ensure secure design and ongoing performance	▪ Finance-facing AI tools — like fraud detection, credit models, or expense automation — may be considered high-risk ▪ Cybersecurity is no longer just an IT responsibility — it's integrated into governance and audit readiness

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Risk-based Classification Framework

- Four risk categories:
  - Unacceptable Risk: Prohibited outright, such as systems causing harm through manipulation
  - High Risk: Stringently regulated, such as AI in financial decision-making
  - Limited Risk: Subject to transparency obligations
  - Minimal or No Risk: Low-impact AI systems exempt from most obligations
- Purpose of classification:
  - Ensures proportionate regulation based on potential harm

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Examples of High-risk AI Use in Finance

- Fraud detection and transaction monitoring:
  - Involves real-time decisions and behavioral profiling; may affect account access or trigger alerts
- AI in credit, loan, or insurance decisions:
  - Impacts consumer rights and financial inclusion; subject to fairness, explainability, and auditability
- Expense, payroll, and tax automation tools:
  - Affects financial disclosures, compensation accuracy, and regulatory filings; often integrated into financial systems

SURGENT ACCOUNTING & FINANCIAL EDUCATION

What Triggers Oversight for U.S. Firms?

Cross-border exposure triggers compliance

Applies if your AI systems process data from EU citizens or are deployed in the EU

Scenarios that require attention

U.S. tools used by EU clients or subsidiaries

Vendors based in the EU providing AI functionality

Joint ventures or shared platforms involving EU markets

EU AI Act Rollout Timeline and Global Ripple Effects

- Key implementation dates:
  - Feb 2025: Prohibited systems banned; AI literacy obligations apply
  - Aug 2026–2027: Most high-risk AI requirements take effect
- Why it matters for U.S. finance teams:
  - Anticipate vendor certifications, system redesigns, and audit trail obligations
  - EU model influencing emerging AI regulations worldwide

GDPR Overview – Cybersecurity Focus

What Is GDPR?	Cybersecurity Implications for Finance and Accounting	Key GDPR Cybersecurity Practices
▪ The General Data Protection Regulation (GDPR) is a comprehensive data privacy law that applies to any organization handling data from EU citizens	▪ Protecting personal data: finance and accounting professionals can help ensure that all client data, including financial information, is securely stored and processed ▪ Data breach notifications: GDPR requires organizations to report data breaches within 72 hours of discovery	▪ Data minimization and encryption: collect only necessary data and encrypt sensitive information ▪ Access controls: limit access to personal data to authorized personnel ▪ Regular audits: perform audits to ensure compliance with GDPR's cybersecurity requirements

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Key GDPR Cybersecurity Practices for Finance Systems

- Data minimization and encryption:
  - Collect only essential personal or financial data to reduce breach exposure
  - Encrypt sensitive data at rest and in transit to protect confidentiality
- Access controls and role-based permissions:
  - Ensure only authorized personnel have access to client or payroll data
  - Regularly review and revoke unused accounts or outdated permissions
- Audit and breach response protocols:
  - Establish audit trails for data access and changes
  - Implement rapid breach response workflows to meet 72-hour notification requirement

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Emerging Cybersecurity Trends in Global Data Regulation

Expansion of global cybersecurity laws	Nations are enacting data protection and breach notification laws beyond the EU U.S.-based organizations must monitor laws like Brazil's LGPD, Canada's PIPEDA, and India's DPDP Act
Cross-border data and cloud security requirements	Regulations increasingly require data localization, encryption, and access transparency Financial platforms must secure cloud infrastructure across jurisdictions
Implications for U.S. accounting and finance professionals	Financial systems handling personal or transaction data face growing regulatory scrutiny Cyber compliance is becoming a board-level responsibility in multinational operations

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Aligning U.S. Financial Cybersecurity Programs with Global Compliance Trends

U.S. regulations are evolving alongside global cybersecurity laws	SEC rules now require cyber risk disclosure and incident reporting Gramm-Leach-Bliley Act (GLBA) and FFIEC guidelines emphasize data security in financial institutions
Aligning with global frameworks strengthens enterprise readiness	GDPR, Brazil's LGPD, and other global standards influence vendor risk, data handling, and breach response Adopting global best practices promotes consistency across controls and audit documentation
Financial professionals play a key role in cyber compliance strategy	Oversee internal controls involving cloud apps, financial data, and third-party access Coordinate across departments to ensure risk documentation meets global expectations

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Chat Prompt

Think about one key vendor you rely on (e.g., payroll, finance software, data storage). Do you know if they comply with GDPR or international breach rules? Should you?

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Analyze financial impacts from cybersecurity breaches using real-world case studies

Image generated by OpenAI's DALL·E through ChatGPT

Cybercrime Losses Reported to the FBI Internet Crime Complaint Center (IC3)

Total complaints

859,532[1]

Volume of cyber incidents reported to the FBI by U.S. victims

Verified losses

$16.6 billion[1]

Record high — funds wired, stolen, or paid

Average loss per case

$19,372[1]

Even relatively small incidents can disrupt cashflow for small and medium sized businesses

Takeaway for financial professionals: FBI numbers are a floor, not a ceiling – many victims never file, so true losses are higher

1. Source: FBI Internet Crime Complaint Center (IC3), *2024 Internet Crime Report*, pp. 4-5. (https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf) Figures represent cyber incidents **reported to the FBI by U.S. victims** in 2024. Global losses are higher because many incidents outside the U.S.—or unreported domestically—are not included.

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Financial Fallout of a Cyber Breach – A Lifecycle View

Stage 1: Detection and Containment

- Breach detected by IT/security team
- Initial investigation and system isolation
- Finance supports resource allocation, tracks early costs

Stage 2: Financial Assessment and Reporting

- Direct losses: stolen funds, legal fees, client refunds
- Indirect losses: downtime, reputational damage, regulatory exposure
- Finance estimates losses and prepares disclosures

Stage 3: Disclosure and Remediation

- SEC Form 8-K (material incidents within 4 days), GDPR/GLBA triggers
- Recovery spending, insurance filing, audit remediation
- Finance coordinates cross-functional communication and recovery budgets

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Case Study – MOVEit File Transfer Breach

- Global software supply chain vulnerability:
  - Exploited vulnerability in Progress Software's MOVEit file transfer app[1]
  - Affected 2,500+ organizations across finance, education, and healthcare sectors[2]
- Third-party risk: hidden dependencies:
  - Breach reached organizations via vendors and contractors using MOVEit
  - Many victims were unaware they relied on MOVEit until after the compromise
- Financial consequences for victims:
  - Legal costs, regulatory filings, and breach notification obligations
  - Long-tail expenses: class-action lawsuits, reputational damage, cyber insurance premiums

1. Source: https://www.ncsc.gov.uk/information/moveit-vulnerability
2. Source: https://www.nccgroup.com/us/newsroom/reflections-on-the-moveit-data-breach-a-year-on/

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Case Study – MGM Resorts Cyberattack

- Social engineering takedown:
  - Attacker posed as an employee and tricked IT help desk into resetting credentials
  - Breach affected digital hotel check-in, slot machines, and payment systems
- $100M+ in estimated damages[1]:
  - Revenue disruption from halted operations across hospitality infrastructure
  - Additional costs for forensics, PR, and accelerated security rollout
- Internal control weaknesses exposed
  - No identity verification protocol at help desk enabled access escalation
  - Post-incident investment in MFA, call verification scripts, and zero trust access

1. Source: Zeba Siddiqui, "Casino giant MGM expects $100 million hit from hack that led to data breach." Reuters, 5 Oct 2023. https://www.reuters.com/business/mgm-expects-cybersecurity-issue-negatively-impact-third-quarter-earnings-2023-10-05/

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Sector-specific Losses – Financial Services

- Financial services: high cost, high stakes:
  - $6.08M[1] average breach cost in financial sector
  - Frequent regulatory audits, extensive data sensitivity
- Common breach vectors:
  - Credential stuffing, phishing, and vulnerable APIs
  - Often linked to remote access tools and vendor integrations
- Impacts on financial reporting and compliance:
  - Potential liabilities, impairment losses, and reserve adjustments
  - Heightened scrutiny from regulators, boards, and rating agencies

1. Source: *Cost of a Data Breach Report 2024*. IBM Corporation. Retrieved from https://www.ibm.com/reports/data-breach

Breach Cost Variables

- What drives breach costs up:
  - Delays in detection (MTTD) and containment (MTTR)
  - Lack of automation, outdated patching processes, and manual logging
- What reduces breach costs:
  - AI-enabled detection reduces breach lifecycle by up to 100+ days
  - Tabletop exercises improve coordination and reduce downtime and chaos
- Role of finance in managing costs:
  - Track cross-departmental breach costs: IT, HR, legal, communications
  - Prepare models for insurance claims, reserve adjustments, and disclosures

Cyber Insurance and Breach Cost Recovery

- What cyber insurance typically covers:
  - Legal costs, breach notification, forensics, and credit monitoring
  - Some policies include PR services and data recovery reimbursements
- Where coverage falls short:
  - Exclusions for poor controls, delayed reporting, or 'nation-state' attribution
  - Disputes over whether ransomware or negligence triggered breach
- Finance's role in recovery:
  - Maintain documentation for every dollar spent during response
  - Collaborate with brokers to ensure claims are substantiated and timely

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Accounting and Finance's Role in Breach Management

- Cyber risk = financial risk
  - Breaches can create material liabilities, disrupt cash flow, and impact earnings
  - Finance must help assess impact and participate in executive response
- Finance as a core incident response partner:
  - Model financial losses, support regulatory disclosures, document breach costs
  - Lead insurance claims, reserve creation, and stakeholder communication
- What financial professionals should do next:
  - Join tabletop exercises and breach simulations
  - Reassess third-party contracts, control narratives, and incident playbooks

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Discussion Prompt

Your payroll system is hit by ransomware on Wednesday — payday is Friday

What steps would your finance or HR team take to make sure employees are paid on time?

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Apply cybersecurity policies and controls that align with U.S. regulatory frameworks while addressing global compliance trends

Image generated by OpenAI's DALL·E through ChatGPT

Cybersecurity Compliance – A Strategic Finance Priority

Cybersecurity policies now shape financial compliance:	Cross-border operations add regulatory complexity:	Finance must apply cybersecurity policies with intent:
▪ Finance must ensure that systems supporting financial reporting meet regulatory expectations ▪ SEC, GLBA, and SOX require verifiable controls for access, data integrity, and disclosure timeliness	▪ Global finance functions face overlapping cybersecurity obligations across jurisdictions ▪ U.S. rules often conflict with GDPR, ISO 27001, DORA, and sector-specific global mandates	▪ Involves more than approving budgets — includes policy enforcement, control testing, and documentation ▪ Examples: validating segregation of duties in ERP systems, ensuring vendor contracts include breach terms

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Key U.S. Cybersecurity Regulations Impacting Accounting and Finance

- SEC cyber disclosure rule:
  - Public companies must disclose material cyber incidents within 4 business days (Form 8-K)[1]
  - 10-K requirements for describing cyber risk oversight and governance
- Gramm-Leach-Bliley (GLBA) Act Safeguards Rule:
  - Requires financial institutions and service providers to maintain written cybersecurity programs
  - Finance teams must ensure vendors handling sensitive data comply with security and breach response requirements
- SOX Section 404 – internal controls over financial reporting (ICFR):
  - IT systems that impact financial reporting are included in ICFR scope
  - Cybersecurity-related controls will likely need to be evaluated

1. U.S. Securities and Exchange Commission, Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release No. 33-11216 (Aug. 1, 2023), https://www.sec.gov/files/rules/final/2023/33-11216.pdf

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Core Cybersecurity Controls Accounting and Finance Should Know

- Access controls – who has access to what?
  - Enforce least-privilege access across financial systems like ERP, AP, and payroll
  - Regular access reviews and dual-approval processes are key control activities
- Monitoring and alerting for financial systems:
  - System logs should capture high-risk transactions and changes to key financial data
  - Alerting should trigger for anomalies like off-hours access or unauthorized data exports
- Data protection and classification:
  - Encrypt financial data and personally identifiable information (PII) at rest and in transit
  - Classify sensitive data to guide retention, deletion, or breach escalation procedures

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Accounting and Finance-owned Responsibilities in Cyber Policy Execution

Risk Registers and Internal Control Mapping	Third-party Risk and Vendor Governance	Policy Enforcement and Expense Oversight
▪ Document cyber risks related to financial reporting, payments, and compliance ▪ Align risk statements with COSO and NIST frameworks to support audits and disclosures	▪ Ensure vendors provide SOC reports or cybersecurity certifications (e.g., ISO 27001, PCI DSS) ▪ Include breach notification clauses, liability language, and security controls in contracts	▪ Finance plays a role in monitoring cybersecurity spend and validating alignment with policy objectives ▪ Ensure incident response and recovery costs are tracked for insurance claims, audit readiness, and financial impact disclosures

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Connecting COSO Internal Controls to Cybersecurity

Control Environment – Culture and Tone at the Top	Risk Assessment – Cyber Risk as a Financial Exposure	Control Activities – Operationalizing Policies
▪ Leadership must embed cyber risk into financial governance and ethical culture ▪ Finance teams help model accountability for data integrity and policy compliance	▪ Include cyber threats in the enterprise risk assessment process (e.g., ransomware, data leaks) ▪ Map risks to likelihood and impact — including potential for restatements or delayed filings	▪ Implement role-based access, dual approval, and review workflows for finance systems ▪ Use technology (e.g., audit logs, automated alerts) to enforce controls and flag violations

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Applying NIST Cybersecurity Framework (CSF) 2.0 to Accounting and Finance

- Overview: NIST Cybersecurity Framework (CSF) 2.0:
  - Six functions: govern, identify, protect, detect, respond, recover
  - Adopted by federal agencies and many private companies for cyber risk management
- Finance-relevant applications:
  - "Identify" financial data assets and who has access (GL, payroll, treasury systems)
  - "Protect" with encryption, multi-factor authentication, and logical segregation
- Benefits for accounting and finance teams:
  - Promotes standardized, auditable cybersecurity practices across departments
  - May support documentation required for SOX, GLBA, and cyber insurance underwriting

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Bridging U.S. and Global Frameworks

- GDPR – security and privacy for EU data:
  - U.S. finance teams handling EU customer or employee data must meet GDPR standards
  - Includes breach notification within 72 hours and data minimization principles
- EU AI Act and DORA – emerging cyber standards:
  - EU AI Act requires cybersecurity controls for high-risk AI use in finance (e.g., credit scoring)
  - DORA mandates resilience testing, vendor risk oversight, and incident classification
- International standards Like ISO 27001 and SOC 2
  - ISO 27001 provides a globally recognized security framework
  - SOC 2 is used in the U.S. but also helps demonstrate alignment with international controls

SURGENT ACCOUNTING & FINANCIAL EDUCATION

U.S.–Global Cyber Policy Misalignments

- Conflicting breach notification requirements:
  - SEC: 4 business days for material incidents (Form 8-K)
  - GDPR: 72-hour breach notification rule for EU data controllers
- Different standards for risk and materiality:
  - U.S.: Focus on investor impact and financial statement risk
  - EU: Emphasizes individual data rights, privacy impact, and harm to subjects
- Record retention vs. minimization mandates:
  - SOX and SEC may require long-term audit logs and control documentation
  - GDPR emphasizes data minimization and deletion obligations
  - **Retention clash example:** SOX § 802 forces 7-year storage of audit/security logs, while GDPR's "right to erasure" limits keeping personal data — requiring pseudonymized or split-storage log solutions to satisfy both rules

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Best Practices for Global Compliance Alignment

- Unified cyber policy framework with flexibility:
  - Base core policies on COSO and NIST for consistency
  - Layer in regional annexes for GDPR, DORA, and state-level rules
- Cross-functional governance and ownership:
  - Involve legal, compliance, IT, and finance in policy lifecycle
  - Assign ownership for contracts, data flows, and breach escalation by jurisdiction
- Routine third-party risk and contract reviews:
  - Reassess vendor contracts annually for cross-border compliance alignment
  - Confirm breach reporting obligations, indemnity clauses, and SLA enforcement

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Case Study – Global Policy Misalignment (LinkedIn)

- Incident summary:
  - LinkedIn fined €310M by Ireland's Data Protection Commission[1]
  - Found to be using personal data for advertising without lawful GDPR basis
- Breakdown: disconnect between U.S. and EU policies:
  - Global ad strategy not aligned with GDPR consent requirements
  - Financial impact wasn't adequately disclosed ahead of enforcement
- Accounting and finance takeaways:
  - Global policy alignment is a finance-level issue: disclosures, reserves, and liability exposure
  - Risk registers should include regulatory divergence and policy gaps as real risks

1. Source: Irish Data Protection Commission, "Irish Data Protection Commission fines LinkedIn Ireland €310 million," Press Release, 24 Oct 2024. https://www.dataprotection.ie/en/news-media/press-releases/irish-data-protection-commission-fines-linkedin-ireland-eu310-million

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Chat Prompt

Think about one finance-related system, process, or vendor your team uses regularly

Is there a cybersecurity control, disclosure process, or vendor policy that may be outdated or misaligned with current regulations — either U.S. or international?

SURGENT
ACCOUNTING & FINANCIAL EDUCATION

Reflection Activity

Image generated by OpenAI's DALL·E through ChatGPT

Reflection Activity

- Think about your current role and responsibilities. After completing this course, what's one cybersecurity policy, control, or compliance area that you now feel more equipped to evaluate or improve?
- You might reflect on:
  - A risk mitigation strategy you'd like to apply
  - A compliance requirement that now feels clearer
  - A vendor or system you plan to re-assess
  - A new conversation you'll initiate with your IT, audit, or legal team

SURGENT ACCOUNTING & FINANCIAL EDUCATION

Learning Objectives

- Identify essential components of a cybersecurity risk management program, including policies and controls
- Evaluate cybersecurity risks and develop risk mitigation strategies tailored for financial professionals
- Understand global compliance standards, such as the EU AI Act and GDPR, and their implications for U.S.-based organizations
- Analyze financial impacts from cybersecurity breaches using real-world case studies
- Apply cybersecurity policies and controls that align with U.S. regulatory frameworks while addressing global compliance trends

SURGENT ACCOUNTING & FINANCIAL EDUCATION