Cybersecurity Governance: Where Do Good Boards Go Wrong?

March 2025

Poll #1:

As a board member, are you aware and knowledgeable about your company's top cybersecurity risks?

Yes
No
Unsure

Emerging industry-specific issues to incorporate into enterprise-wide cybersecurity programs: *(Courtesy of ChatGPT and BDO cyber subject matter professionals)*

Technology	Financial Services	Retail & Consumer Products	Healthcare	Manufacturing
✅AI-Powered Attacks – Use of deepfakes, AI-driven phishing, and automated hacking tools to compromise systems. ✅ Software Supply Chain Vulnerabilities – Risks from third-party vendors, open-source components, and compromised software updates (e.g., SolarWinds-style attacks). ✅ Cloud Security & Zero Trust Adoption – Threats targeting multi-cloud environments and misconfigured identity access controls. ✅ Data Privacy & Regulatory Complexity – Compliance with evolving global data protection laws (GDPR, CCPA, China's PIPL). ✅ Intellectual Property Theft & Espionage – Targeting of patents, source code, and proprietary R&D by cybercriminals and nation-states.	✅ Real-Time Payment Fraud & Deepfake Scams – Cybercriminals using synthetic identity fraud and AI-generated voices for unauthorized transactions. ✅ Ransomware Disrupting Critical Financial Infrastructure – Attacks on core banking systems, ATMs, and payment processing networks. ✅ Third-Party Risk in FinTech & Banking-as-a-Service (BaaS) – Exposure to cyber threats from outsourced banking services and API integrations. ✅ Regulatory Reporting & Incident Disclosure Compliance – SEC, FFIEC, and global regulators mandating real-time breach notifications and cyber resilience testing. ✅ Quantum Computing Threats – Future risks of post-quantum cryptographic attacks against encryption in financial transactions.	✅ E-Commerce & Credential Stuffing Attacks – Large-scale automated bot attacks targeting customer accounts and loyalty programs. ✅ Point-of-Sale (POS) & Payment Card Data Breaches – Malware targeting POS systems and mobile payment applications. ✅ Omnichannel Fraud (Online & In-Store) – Integration risks between physical retail, digital storefronts, and mobile commerce. ✅ Fake Reviews & Social Engineering Scams – AI-generated fake product reviews, phishing scams impersonating brands. ✅ Third-Party Logistics & Supply Chain Attacks – Cyber risks affecting warehousing, shipping, and fulfillment partners.	✅ Ransomware Targeting Hospital Systems – Attacks disrupting electronic health records (EHR), telemedicine platforms, and medical devices. ✅ Medical Device Hacking & IoT Vulnerabilities – Exploitation of networked pacemakers, insulin pumps, and imaging systems. ✅ Data Integrity & AI in Diagnostics – Risks of manipulated AI-driven diagnoses and altered patient health records. ✅ HIPAA & Patient Privacy Compliance – Increasing regulatory enforcement of breach reporting and third-party security obligations. ✅ Pharmaceutical & Biotech IP Theft – Cyber espionage targeting drug research, vaccine development, and clinical trials.	✅ Industrial Control System (ICS) & Operational Technology (OT) Attacks – Exploits targeting SCADA systems and factory automation. ✅ Ransomware in Smart Factories – Disruptions to robotics, AI-driven production lines, and just-in-time (JIT) supply chains. ✅ IP Theft & Counterfeit Goods Risks – Cyber espionage targeting engineering blueprints, 3D printing files, and trade secrets. ✅ Third-Party Risk in Component Suppliers – Attacks on embedded firmware, chips, and semiconductor suppliers. ✅ Regulatory & Compliance Mandates (CMMC, NIST 800-171) – Increasing cybersecurity requirements for defense and aerospace manufacturers.

Emerging industry-specific issues to incorporate into enterprise-wide cybersecurity programs: *(Courtesy of ChatGPT and BDO cyber subject matter professionals)*

Transportation & Logistics	Energy & Utilities	Food & Beverage	Education	Hospitality
✅ Maritime & Aviation Cybersecurity – Threats targeting GPS spoofing, ship navigation systems, and airline reservation platforms. ✅ Ransomware Disrupting Global Supply Chains – Attacks on port authorities, freight companies, and rail operators. ✅ Fleet & Vehicle Cybersecurity – Risks in connected vehicles, autonomous trucking, and drone logistics systems. ✅ IoT Risks in Smart Ports & Airports – Cyber vulnerabilities in automated container terminals, baggage handling, and customs processing. ✅ Cyber-Physical Risks in Rail & Mass Transit – Increasing threats to train control systems, ticketing platforms, and urban transit infrastructure.	✅ Critical Infrastructure Cyberattacks (Nation-State & Ransomware) – Threats to power grids, oil pipelines, and water treatment facilities. ✅ SCADA & Industrial Control System (ICS) Security – Legacy system vulnerabilities in electric, gas, and water utilities. ✅ Cyber Risks in Renewable Energy (Wind, Solar, EV Charging Stations) – Exploits targeting distributed energy resources and smart grids. ✅ Physical & Cyber Threat Convergence – Hybrid attacks combining cyber intrusions with physical sabotage of power stations. ✅ Cyber Resilience & Government Regulations (NERC CIP, CISA, DOE) – Increasing regulatory scrutiny over grid security and blackout prevention.	✅ Food Supply Chain Cyber Risks – Disruptions in agriculture, processing plants, and distribution networks due to cyberattacks. ✅ Ransomware in Food Manufacturing & Retail – Targeting of automated processing facilities and grocery POS systems. ✅ Tampering & Food Safety IoT Vulnerabilities – Cyber threats to automated temperature control, food safety monitoring, and blockchain traceability. ✅ Third-Party Risk in Restaurant & Delivery Platforms – Data breaches affecting online food ordering services and gig-economy delivery networks. ✅ Regulatory & Compliance Pressures (FSMA, FDA, USDA) – Increasing cybersecurity expectations for food safety, supply chain transparency, and traceability.	✅ Ransomware Attacks on Universities & K-12 Schools – Disruptions to online learning, research, and administrative systems. ✅ EdTech & Student Privacy Risks – Compliance challenges with FERPA, GDPR, and cloud-based learning platforms. ✅ Phishing & Credential Theft – Targeted attacks on faculty, students, and research data. ✅ AI-Generated Exam Fraud – Use of deepfake and AI tools for academic dishonesty. ✅ Cyber Espionage in Research Institutions – Government-sponsored hacking of university research programs.	✅ Guest Data & Loyalty Program Breaches – Theft of personal and payment data from hotel chains, airlines, and travel platforms. ✅ Smart Hotel & IoT Security Risks – Vulnerabilities in smart locks, room automation systems, and mobile key access. ✅ Online Booking Fraud & Fake Travel Websites – Phishing schemes targeting customers making hotel or airline reservations. ✅ Wi-Fi & Guest Network Attacks – Exploitation of public Wi-Fi networks in hotels and airports for man-in-the-middle attacks. ✅ Cyber-Physical Security Convergence – Integration risks between physical security (CCTV, access control) and IT systems.

Emerging industry-specific issues to incorporate into enterprise-wide cybersecurity programs: *(Courtesy of ChatGPT and BDO cyber subject matter professionals)*

Gaming	Professional Sports	Entertainment	Mining	Nonprofits
✅ Account Takeovers & Credential Theft – Large-scale hacks targeting player accounts, in-game currency, and NFTs. ✅ DDoS Attacks on Multiplayer Servers – Cybercriminals disrupting online gameplay and esports competitions. ✅ In-Game Fraud & Microtransaction Exploits – Hacking of virtual goods, loot boxes, and digital marketplaces. ✅ Cheating Tools & AI-Assisted Hacking – Use of AI bots and machine learning to create undetectable hacks. ✅ Privacy & Data Breaches in Gaming Platforms – Risks in voice chat recordings, player behavior tracking, and stored payment data.	✅ Player & Team Data Security – Theft of biometric performance data and proprietary analytics. ✅ Ticketing & Fan Engagement Cyber Risks – Phishing and fraud targeting online ticket sales and mobile apps. ✅ Streaming & Piracy Threats – Cybercriminals exploiting illegal sports streaming services and content theft. ✅ Stadium & Event Security – Cyber-physical threats to smart stadiums, connected security systems, and live event networks. ✅ Sponsorship & E-Sports Fraud – Cyber threats impacting digital sponsorship deals and virtual gaming platforms.	✅ Streaming Piracy & Content Theft – Illegal distribution of movies, TV shows, and live performances. ✅ Deepfake & AI-Generated Fraud – AI-driven manipulation of celebrity endorsements, voice cloning, and fake videos. ✅ Leaks of Unreleased Content – Cyberattacks targeting production studios, music labels, and digital archives. ✅ Social Media Account Takeovers – Hacking of high-profile entertainers' accounts for scams or misinformation. ✅ Fan Data & Subscription Platform Breaches – Cyberattacks on OTT platforms, ticketing services, and fan engagement apps. ✅ Cybersecurity in Live Events & Productions – Threats to digital assets, remote editing workflows, etc.	✅ Cyber Threats to Autonomous Mining Equipment – Hacking of automated drills, haul trucks, and remote-controlled machinery. ✅ Operational Technology (OT) & Industrial Control System (ICS) Attacks – Exploits targeting SCADA systems in mines. ✅ Ransomware Targeting Extraction & Processing Facilities – Disruptions to refining, smelting, and mineral transportation. ✅ Supply Chain Cyber Risks in Resource Extraction – Attacks on logistics partners and third-party vendors. ✅ Geospatial & Exploration Data Theft – Cyber espionage targeting proprietary geological surveys and exploration data. ✅ Regulatory Compliance & ESG Cyber Risks – Ensuring cybersecurity aligns with environmental, social, and governance (ESG) standards.	✅ Donor Data & Financial Fraud Risks – Attacks on fundraising platforms and donor databases. ✅ Cybersecurity Gaps in Small NGOs – Limited budgets making nonprofits attractive cyber targets. ✅ Nation-State Espionage Targeting Advocacy Groups – Political hacking and surveillance risks. ✅ Disinformation & Social Media Attacks – AI-generated misinformation campaigns targeting nonprofit causes. ✅ Third-Party Vendor Risks – Cyber threats from outsourced IT and payment processing providers.

Poll #2:

How frequently does your board discuss the consistency of your internal and external documentation with respect to the board's and management's responsibilities for technology and cyber risks? Especially as they relate to your top cyber risks.

Annually
Quarterly
Only as needed
N/A

SEC Cybersecurity Risk Management, Strategy & Governance Final Rules

Item	Disclosure Requirement
New Regulation S-K Item 106(1) - Definitions	• **Cybersecurity incident:** An unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein. • **Cybersecurity threat:** Any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity or availability of a registrant's information systems or any information residing therein. • **Information systems:** Electronic information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations.
New Regulation S-K Item 106(b) - Risk Management and Strategy	Describe processes, if any, for the assessment, identification, and management of **material** risks from cybersecurity threats, and describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition.
New Regulation S-K Item 106(c) - Governance	Describe **board's oversight** of risks from cybersecurity threats: • Identity any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats. • Processes by which the board or such committee is informed about such risks.
New Regulation S-K Item 106(c) - Governance	Describe **management's role** in assessing and managing material risks from cybersecurity threats, including (non-exclusive list): • Whether and which management committees or positions are responsible for assessing and managing such risks, and the relevant expertise of such persons or members. • Processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents. • Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.

Exercise

AUDIT COMMITTEE DOCUMENTS	PROXY STATEMENT	10-K ITEM C EXCERPT	10-K RISK FACTOR EXCERPTS
Charter: *"The Audit Committee assists the board in overseeing and monitoring the Company's cybersecurity risk management strategies."* ***AC Agenda:*** *XX/XX/XXX agenda reflected time allocated to cyber update and desktop exercise*	"Board member X has broad experience across the finance function including… cybersecurity and system implementations …"	"Our Board of Directors oversees our overall risk management strategy. Our information security program is managed by a dedicated Head of Information Technology [HoIT], who has over twenty years of experience in IT…. Our program is assessed both internally and externally by third parties… Our [HoIT] provides reports at least quarterly to our Audit Committee, as well as our Disclosure Committee… The reports provided include updates on our cyber risks and threats, key updates to our information security systems and programs as well as the current threat environment."	"We rely on technology in our business and any cybersecurity incident, other technology disruption or delay in implementing new technology could negatively affect our business and our relationships with customers…"

SEC Comment Letters: Item C Cybersecurity

As of November 30, 2024: Five comment letters from the SEC Staff regarding disclosure under Item 1C.

- Two letters requested companies refile annual reports to include an omitted Item 1C. Companies filed an amendment on Form 10-K/A, adding requested disclosure.
- One letter requested company amend future filings to clarify inconsistent statements about its engagement of 3rd parties in connection with its processes for identifying, assessing and managing material risks from cybersecurity threats. Company clarified nature of its engagement of 3rd parties in identifying and managing cybersecurity risks, confirming it would clarify this point to avoid any inconsistency or ambiguity in future filings.
- Three comment letters, SEC Staff touched on Item 106 requirements, requesting expanded disclosure in future filings:
  - **Item 106(b)(1) (*Processes for Assessing, Identifying, and Managing Material Risk from Cybersecurity Threats*).** Requested expanded disclosure to describe areas of responsibility of its executive management team and board, along with their respective processes in response to this disclosure item. Company confirmed it would include the requested detail in future filings.
  - **Item 106(b)(1)(i) (*Integration of Cybersecurity Risk Processes into Overall Risk Management*).** In one comment letter, requested revision to future filings to disclose how processes for "assessing, identifying, and managing" material cybersecurity threats have been integrated into its overall risk management system or processes in response to this disclosure item. Company emphasized these processes are "well integrated" into its overall risk management system, noting relevant disclosure included in its current filing, and agreeing to provide more detail in future filings in response to this disclosure item.
  - **Item 106(c)(2)(i) (*Identification of Management Committees or Positions Responsible for Assessing and Managing Material Risks from Cybersecurity Threats*).** Two comment letters noted above also included comments related to the discussion of management's responsibility over cybersecurity risks. The first requested company identify which management positions or teams are responsible for assessing and managing material risks from cybersecurity threats in future filings. The second requested discussion of the relevant expertise of the company's senior leadership responsible for managing the company's cybersecurity risk and the "design and implementation of policies, processes and procedures to identify and mitigate this risk." In each case, the company confirmed it would include the requested detail in future filings.

Source: https://www.gibsondunn.com/cybersecurity-disclosure-survey-of-form-10-k-cybersecurity-disclosures-by-sp-100-cos/

Group Exercise

Scenario:

As a member of the board, you just received a text from your CFO indicating that a cyber incident involving a third-party vendor could potentially involve certain sensitive data belong to your company.

Instructions:

Thinking about your own organization's cyber incident response plan, consider the question assigned to your table and identify practices to share with the broader group:

Group Scenario Exercise (cont'd)

Questions

1. How has your board and management team specifically discussed/defined the conditions that may lead to a conclusion that a cyber incident would be considered 'material' to the business?
2. Think about the last time the board and management reviewed your incident response plan. What do you consider to be the better practices your organization has adopted (or perhaps should adopt) when performing such reviews?
3. As it relates specifically to cyber vulnerabilities created through engagement with 3rd parties, what does your board expect of your management team and advisors to mitigate such risks?
4. Reflecting on some of the highlights from our earlier discussion and/or publicly reported cyber incidents, are there recognizable gaps or areas within your cybersecurity risk oversight and management that you intend to raise at your next board meeting (if not sooner)?

Group Exercise

Scenario: An hour later, the CFO updates the board that upon further investigation by the CISO's team and communications with the third party vendor, the company believes that confidential information of an unknown number of its clients has been accessed by hackers that may be related to a failure of a security patch on the part of the 3rd party and neither the company nor the 3rd party is able to access any client data as it has been encrypted. The company has just received a ransom request for $10M for the data to be reinstated and not shared further. The company has 48 hours to comply with the ransom demand.

Group Exercise

Poll:

Given this scenario, and thinking as an individual director, would you advise leadership to pay the ransom?

Yes

No

Unsure

Group Exercise

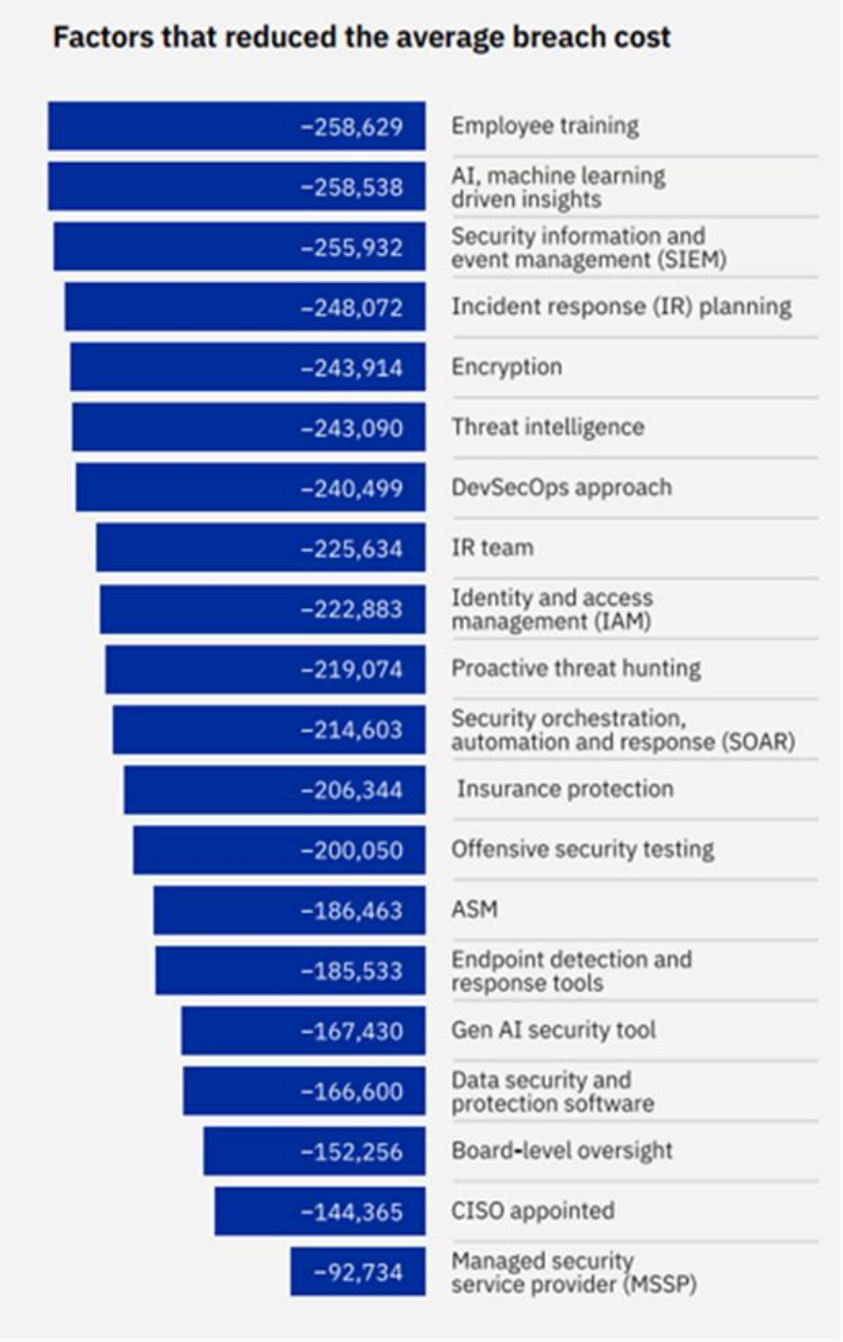
Question:

In your groups, break down what specific elements of a cyber incident response plan would best assist your board and management team in determining appropriate steps to take.

Consider:

- If YES would pay, what are the pros/cons in doing so?
- If NO, why do you feel this way and what strengths in your cyber incident response plan are you relying on?
- If UNSURE, what should be the key aspects you may need to think about?

Actions to Reduce Average Breach Cost



Source: [Cost of a Data Breach Report 2024]

About BDO USA

At BDO, our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes — for our people, our clients and our communities. Across the U.S., and in over 160 countries through our global organization, BDO professionals provide assurance, tax and advisory services for a diverse range of clients.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C, a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

www.bdo.com