ZURICH

Cyber resilience
Preparing risk executives for cyber incidents

Cyber Risk Management
Zurich Resilience Solutions

Contents

I. Introduction

If cybersecurity was once the sole domain of Information Technology (IT), the goal today is cyber resilience, often shared by Information Security (i.e., the Chief Information Security Officer), Risk Management, Legal and others. The stakes are high, from business impact of malware to crippling supply chain attacks and stringent regulatory requirements. Risk Managers now find themselves involved in (and sometimes overseeing) a highly technical discipline, often without being equipped with the necessary information and tools to be effective.

This paper will outline the basics for Risk Managers and other corporate leaders. While Chief Information Security Officers (CISOs) may provide primary protection and response to the organization, the strategy and execution of Risk Managers and other business leaders will help determine the survival and continuity of the company. Therefore, it's vital they understand the roles and responsibilities, and prepare adequately for a cyber incident.

In some ways, cyber risk management is no different from any other risk management discipline. ISO 31000, a guide on risk management from the International Organization for Standardization, defines risk as "the effect of uncertainty on objectives,"[1] to reflect that a risk does not purely represent downside potential, but upside if managed appropriately. Cyber risk is a great reflection of this definition — with proper risk management technique, including identification, assessment and treatment, the effects of a cyber risk can have a far smaller impact (and even a substantial upside impact) on the organization's objectives. In fact, when viewed through the lens of risk management instead of just IT, cyber risk can be treated more practically and uniformly, to achieve a true return on investment for the organization.

There are many specific and technical components to a cyber risk management program, but this paper will focus primarily on the incident response function. This blends pre-incident planning and preparation with post-incident actions to achieve the best possible outcome for the organization. As Risk Managers look for ways to add value to the organization by reducing and mitigating cyber risk, the Incident Response Plan (IRP) is an area with clear return on investment. According to a report from IBM Security and Ponemon Institute, the average cost of a data breach in 2024 was $4.88M and that cost was reduced by $192,266 on average when companies endured a breach. This emphasizes the value of training and preparing employees for incidents and how to spot them.[2]

Cybersecurity firm SpearTip of Zurich Resilience Solutions validated from their nearly two decades handling cyber incidents that "organizations with an Incident Response Plan in place identify breaches faster, experience less downtime, and reduce the total cost of a data breach."[3]

Risk Managers have an important role to play in reducing and mitigating cyber risk, and one of the best drivers of ROI for them is in sharpening incident response capabilities.

II. The Risk Manager's role in cybersecurity

This paper is not intended to comprehensively outline the controls and other technical elements of a cybersecurity program, but some of the basics are covered here with the objective of educating risk management leaders to promote effective discussions with the CISO and other technical teams. Furthermore, the evolution of Cybersecurity Risk Management is clearly leading to a stronger role by Risk Managers, in collaboration with Information Security and IT leaders.

The cybersecurity world is littered with lists, frameworks, guidance and acronyms for cybersecurity programs. This includes the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), the Center for Internet Security (CIS) "Top 18" controls, ISO 27001, PCI-DSS, etc. Fortunately, these mostly overlap with one another and need not all be studied in depth. Here we outline the elements NIST 2.0.

It's important that risk managers understand that IT operations inherently present risk. Cyber risk is an often-siloed area due to a lack of familiarity with Information Technology or Information Security concepts. Information Technology is the enabling architecture that most modern business practices are built and operate on. The many frameworks that are discussed above are tools to provide a common language for business professionals and technologists to discuss and plan a strategic approach to controlling the risk that technology presents.

The NIST CSF 1.1[4] is divided into the five functions listed below. Each function has several specific elements, for a total of 23 distinct categories (and further broken down to 108 subcategories). While all have an important role, one category has been identified within each function as particularly important to highlight for a risk executive audience.

Identify: This function involves identifying and understanding assets (e.g., data, hardware, software, systems, facilities, services, people) and the related cybersecurity risks.

- Asset management (otherwise known as asset inventory) is an often-overlooked area and forms the risk management basis. You can't protect properly if you don't know what you have.

Protect: Here the goal is to outline and implement safeguards to help ensure delivery of critical infrastructure services. This includes the "classic" cybersecurity elements, such as network segmentation, encryption, vulnerability management and security awareness training.

- Access control is one of many critical parts of the Protect function but is highlighted because specific tools like multifactor authentication, privileged access management and other permissions-granting features can offer a robust defense from threat actors. While complex in nature, the basic premises can be easily understood and supported by Risk Management.

Detect: This entails enabling the organization to determine if/when a cybersecurity incident may have occurred so appropriate action can be taken. It is widely acknowledged that early detection correlates to lower total costs associated with a breach.

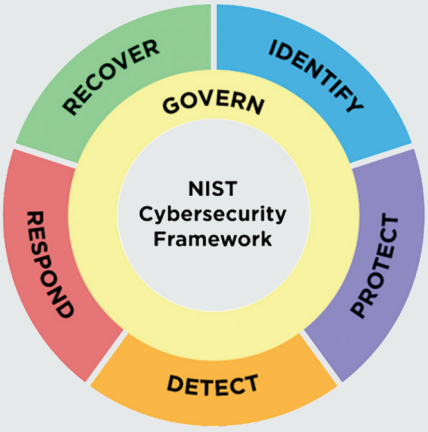
- Security continuous monitoring has proved its value, whether built in-house or, more commonly, outsourced to a 24/7 Security Operations Center as-a-Service (SOCaaS). By combining critical detection and response tools with artificial intelligence (AI) and human-powered analysis, organizations are best protected around the clock, whereas they once were highly vulnerable during non-business hours.

Respond: Often considered the immediate response activities, this function focuses on the organization's containment of the impact from a potential cybersecurity incident to prevent further spread. It involves conducting incident analysis and mitigating effects.

- Response planning is (no surprise, as the core topic of this paper) one of the most vital things that can be undertaken prior to an incident. And like other categories, this is not a tick-the-box exercise – a robust, well-tested IRP will yield benefits unavailable to a less-prepared organization.

Recover: The focus here is on "timely recovery to normal operations to reduce the impact from a cybersecurity incident,"[5] such as system restoration and continued communication and continuity activities.

- Recovery planning often includes data backups, which should be offline and immutable to prevent tampering by threat actors (a go-to move of theirs). While having high-fidelity backups has become ubiquitous, not all organizations have attempted a full failover test and restoration from backup, so while the capability exists theoretically, one cannot be too confident in it. Test your team!



NIST Cybersecurity Framework 2.0 (Public Draft)
Source: National Institute of Standards and Technology

Verify the Sender

In 2024, a healthcare organization suffered a $24 million loss after cyber attackers exploited help desk vulnerabilities to bypass Multi-Factor Authentication (MFA), gain deep internal access, and redirect insurance payments. The attackers manipulated help desk procedures, conducted internal reconnaissance to obtain sensitive financial credentials, and fraudulently altered bank details, resulting in significant financial diversion. The incident highlights the necessity for adaptive identity and access management, AI-driven monitoring to catch anomalies in real time, and ongoing employee training to recognize and resist phishing attempts.

NIST CSF 2.0 added a sixth function: "Govern,"[7] in February of 2024 specifically defined as follows, with underlining added for effect:

> Establish and monitor the organization's cybersecurity risk management strategy, expectations and policy. The Govern function is cross-cutting and provides outcomes to inform how an organization will achieve and prioritize the outcomes of the other five functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management strategy. Govern directs an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policies, processes and procedures; and the oversight of cybersecurity strategy.

To summarize, the first major overhaul of the NIST CSF in 18 years added components that were generated to strengthen the organizational commitment to and embedding of cybersecurity strategy. The objective is to make it less of a purely technical discipline, and more of a business function. This particularly strengthens the involvement of Risk Managers and other risk executives.

III. Incident Response Plan basics

The Incident Response Plan is aptly named to support effective and timely response to a cyber incident. Seems simple enough, so let's keep it that way. A good plan is one that is easy to follow, usable by a variety of individuals, current and reflective of the unique business environment. Great plans are ever-living documents updated frequently based on the evolving business and lessons learned through practical experience. Incredible plans are ones that are discussed and drilled at several levels of the organization, such that the participants feel ready.

A great deal of guidance exists from credible, expert sources, such as NIST, the Cybersecurity & Infrastructure Security Agency (CISA) and others. These entities exist to provide resources to critical infrastructure and other private industry organizations so they can better protect themselves from cyberattacks. The resources are typically provided to eligible entities at no cost, so take advantage!

"... focus on creating a functional, light playbook that is relevant in any scenario"

When setting out to create or enhance a plan for the organization, focus on brevity. A lengthy written plan does not improve outcomes and, in many cases, makes effective response more challenging because teams are combing through pages of guidance to check their intuition. Instead, focus on creating a functional, light playbook that is relevant in any scenario, rather than prescriptive to every conceivable one. Some of the key elements are outlined below.

The plan should have a clear owner — often the head of Information Security or Risk Management — and be shared with key stakeholders. Feedback from non-technical functions like Legal, HR, Operations, Finance, etc. are vital to the plan's health and effective execution if and when it's put into practice. But remember, this is a highly confidential document and should be adequately protected to preserve the organization's response strategy.

The plan also requires an Executive Sponsor, separate and distinct from the functional owner. This individual (ideally C-Suite) provides the authority for the plan, team and associated preparatory actions. The sponsor also helps ensure executive and board-level support of the plan.

The document itself needs to be accessible offline (i.e., printed). In a significant cyber incident, network drives, email and other traditional means of accessing the plan can be unavailable, so it must be easily retrievable by key stakeholders. Maintaining a versioning system is important so that printed copies are kept current.

Consider security and privacy. The IRP should include representation and involvement by Legal counsel to evaluate the potential exposure to data loss and ensure appropriate steps are considered to protect the organization. Methods for investigation and analysis should preserve evidence without increasing exposure. This is where speed must be balanced with an organized and methodical process.

Finally, the plan needs to **have clear testing procedures** (i.e., tabletop exercises outlined below) and established update intervals. These two work together, as "After Action" lessons from simulated exercises, near-misses and real incidents should be incorporated to strengthen the plan over time.

The cyber incident response playbook: Key elements

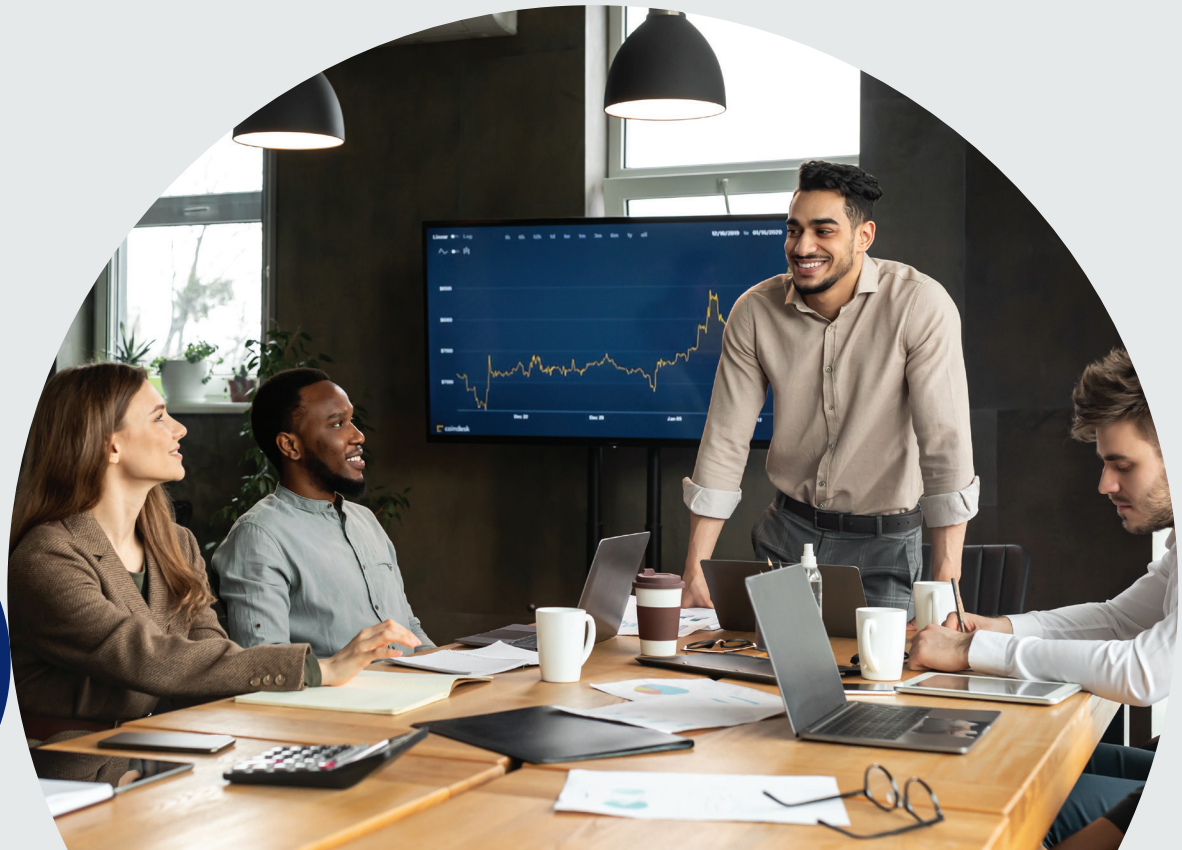
- **Communication methods:** Normal channels (email, video conferencing, etc.) may be unavailable in a cyber incident. A plan needs to outline how the IR team will meet and communicate.
- **Definitions and severity levels:** Very clear and measurable definitions of incident levels must be articulated and included to guide proper response. These should be linked to notification and other initial steps.
- **Team:** The plan should establish the members of the Incident Response team, including the Incident Manager, the single person designated to lead the response efforts.
- **Authority levels:** Determining who has authority to make decisions and take actions is imperative so there isn't confusion or delay.
- **Report and notify:** Clearly outline applicable regulatory reporting requirements, local law enforcement contacts, insurer(s), key customers/vendors, etc. The IRP should merely summarize these as a reference to more in-depth procedures led by Legal or other functions. But this is important so requirements are not overlooked in a potentially high-intensity response scenario.
- **Contact information:** Key internal and external parties should have contact information (and alternate means of contact) listed to facilitate communication and decision-making.

IV. Lessons from tabletop exercises

With a well-written plan in place and relevant internal and external stakeholders a part of it, the organization should commit to exercising the plan. This practice is typically called a tabletop exercise. Tabletop exercises are opportunities for parties represented in the incident response process to simulate and walk through a scenario that the organization may face. Typically, the attendees are composed of one of two groups: technical resources or the executive audience. Tabletop exercises are designed for one of these two audiences because the discussion points and themes are either technical or strategic. To be clear, both are important and have their own value, so organizations should consider both approaches in their annual planning.

It is common to have a third-party facilitator lead the exercise who has significant experience in facilitating effective exercises. While it's possible to organize and lead a tabletop exercise internally, the outside perspective and advice brought by a third party are often valuable.

Many organizations conduct a tabletop cyber exercise at least annually, and often at different levels of the organization, from senior management to IT, to specific business units and geographies. This is a best practice because the drill will expose flaws in the plan that are otherwise not obvious on paper, helping educate participants on their roles, and ultimately save critical time in a real incident.



Over the years, as a third-party facilitator of tabletop exercises, I've observed a few common lessons learned and themes across many organizations, including:

Authority levels need to be more clear: Often, the plan does not specify who has authority to make certain decisions (such as issue a press release, proactively take the network offline, etc.). This is paralyzing to even well-prepared, high-functioning teams, because time is of the essence and the real scenario typically doesn't perfectly reflect the hypothetical one envisioned in the plan. A good plan will tie specific incident levels to delegation in decision-making authority, with alternate approvers established in case the primary is unavailable (e.g., the CFO can act in the absence of the CEO). Can the plan offer a concise answer to "Who's in charge?"

External stakeholders need to be reflected in the plan: In a real scenario, an organization may rely heavily on critical third parties (e.g., Breach Coach/external counsel, Digital Forensics & Incident Responder, Crisis Communications experts, etc.) and also have substantial and time-bound reporting requirements to others (e.g., local, state and/or federal regulators, key customers, insurance carrier, etc.). However, these steps are rarely outlined clearly enough in the plan with contact information and responsibility defined. Can the plan help you answer, at any given time, "Who needs to know?"

Cross-functional representation is often lacking: For understandable reasons, there is a tendency to focus on the information technology / information security resources that will be providing support during an incident. Equally important is the need to have cross-functional representation from Human Resources, Physical Security, Audit, Legal, Communications, Finance and other parties. Their participation in the plan, even if it's a mere notification, enables those with key responsibilities to be informed and, if appropriate, act within their functional responsibilities or contribute to the response.

Continuity of operations needs greater focus: Most IRPs will rightfully focus on the initial hours of the incident, but few will reference a more robust business continuity plan. Cyber incidents have the potential to severely disrupt normal operations for an extended period of time (potentially many weeks). Therefore, while the Incident Response team is focused on stopping the bleeding, another team needs to be thinking a bit longer term on how to recover as much of the organization's mission as possible — and without getting in each other's way. The plan should be able to help you answer, "Once we are back, how will we survive?"

Again, these are common themes and lessons learned, but each organization will benefit in its own way from this exercise. A Risk Manager can sponsor this effort annually, whenever there is material change in the executive team, or after a near-miss incident. Not only will the exercise educate the team and provide essential practice for a real event, but it will also build a bridge from the CISO/IT to the broader company management.

It is invaluable for a company's leadership to go through the process, to fully understand what's at stake and their individual roles in the response. There is simply no substitute for challenging the CEO and executive team with hypothetical consequences and pushing them to evaluate potential response options. That muscle memory can pay dividends.

V. Collaboration with Cybersecurity / Information Technology

Historically, the evolution of the average cybersecurity strategy has gone from non-existent to being siloed with the IT team, to becoming the responsibility of the newly established CISO role, and now being a much more cross-functional discipline with ownership shared by several leaders, including the Risk Manager. Yet another step in the evolution is that public companies will be subject to new SEC rules adopted in July 2023, which require applicable organizations to describe the oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing material risks from cybersecurity threats to the Board of Directors.[8] These shifts reflect the growing magnitude of the risk posed.

Organizations must find the right balance of technical preparedness with organizational processes. This requires the CISO and Risk Manager to navigate ambiguous responsibilities, geographical challenges and an uncertain definition of success. Further complicating matters is that the CISO and Risk Managers typically have very separate reporting structures, so collaboration requires proactivity and effective communication.

Myke Lyons, CISO for cloud-based developer security platform Snyk, said, "CISOs are notoriously armies of one — they have tremendous technical skill and aim those capabilities at highly technical problems. As risks increasingly transcend the security function and threaten investors, customers, employees and others, CISOs must adopt a divide-and-conquer approach. The corporate risk function offers an avenue to magnify the CISO's impact, but the relationship can feel forced at first."[9]

Risk Managers can start building this relationship in ways that are consultative and ease the burden for the CISO, rather than add to it. Here are a few conversation starters for a Risk Manager to consider in their discussions with their organization's CISO or Head of IT:

What's our risk landscape? Risk assessment has long been the domain of the Risk Manager, but by first inquiring about the top risks identified and tracked by the Information Security team, a Risk Manager can educate themselves and demonstrate a collaborative approach. Then they can begin to insert themselves in a measured manner into a critical process, thereby enabling the CISO to focus on strategic execution. Especially in an arena dominated by fast-moving emerging risks, a robust risk identification and assessment process is vital.

Do we have the right insurance? Cyber insurance and other financial risk transfer/funding mechanisms have become core components of a cyber risk management strategy today, yet most CISOs have at best a basic understanding of them. An easy win for a Risk Manager is to lead the marketing of the organization's cyber risk to achieve strong financial protection. This requires building a deeper understanding of the exposures and controls to present to the insurance market. Feedback from carriers and brokers to the Risk Manager can further help the CISO develop the strategic cybersecurity program, and the vendors aligned with the insurance providers can be valuable resources.

Is our cybersecurity budget adequate? A Risk Manager is ultimately responsible for identifying, assessing and quantifying risks to the organization. With cyber risks often being material and potentially ruinous to the organization, a Risk Manager should have senior-level visibility to recommend funding risk management efforts by comparing with other risks across the organization. This can be helpful and form an ethical allyship with a cash-strapped CISO.

Such discussions can be powerful. According to Leslie Lamb, Director of Global Risk Management at Flex, "the Risk Management function is perfectly suited to support and lead cyber risk management alongside CISOs. We often see a hesitancy on both parts, since the risk arena is heavily technical — but driving productive discussions is almost always welcome. Grounding the conversation in organizational objectives helps both parties operate in familiar territory, building trust and growing the impact over time."[10]

VI. Managing up to the board and senior leadership

The Risk Manager and CISO should culminate their progress by reporting up to the Board of Directors and senior management. According to studies cited in Harvard Business Review, "About 47% (of Corporate Boards) believe their organization is unprepared for a cyber attack."[11] Mindful of new SEC reporting requirements, continued headline-making breaches, and other factors, boards will be increasingly demanding of their cybersecurity strategy. Each board will seek its own level and style of reporting from its Risk Management and CISO teams. Ultimately, the goal of the board is to steer and protect the organization, and to do so across a broad base of subjects. Boards will look for simplicity, humility and prioritization in the information they consume from you. Here are a few things to keep in mind:

- **Report consistently:** This includes utilizing the same heat map or other reporting format (ideally consistent with other Risk Management reporting). Also, aim for a consistent cadence of reporting (quarterly or at some other interval).

- **Measure and monitor:** Once through the curiosity of "what if" questions, most boards will look for quantified reporting. This includes risk scenarios distilled to dollar impact or another financial metric, but it should also have risk maturity levels measured as progress over time. Given the audience, these are both good areas to seek independent third-party input and guidance.

- **Know who they know:** This is a bonus one, but most independent directors are well-networked and have a sphere of influence that can be researched or ascertained over time. By knowing what companies they are involved in and where they may typically get their information, you can begin to anticipate questions based on industry events and trends. This level of proactive reporting will instill confidence that Risk Manager and CISO, together, have a steady grasp of the tiller.

This informed, pragmatic and collaborative approach simultaneously shows "we are protecting ourselves as best we can," and "we are as prepared as we can be." Some call this a belt and suspenders approach, and it's very difficult to achieve outside of this cross-functional partnership. Through the aforementioned actions, the CISO and Risk Manager can collectively present a strategy of true cyber resilience that protects their company and reinforces their value to the organization's continued success.

References

1. International Organization for Standardization, ISO 31000:2018 – Risk management. 2021. https://www.iso.org/publication/PUB100464.html
2. IBM Security and Ponemon Institute. "Cost of a Data Breach Report 2025." https://www.ibm.com/reports/data-breach.
3. Kolthoff, Jarrett. Interview. Conducted by David Shluger. 29 August 2023
4. National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.1. 16 April 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
5. National Institute of Standards and Technology. "Special Publication 800-61." https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
6. Kolthoff, Jarrett. Interview. Conducted by David Shluger. 29 August 2023
7. National Institute of Standards and Technology. "Public Draft: The NIST Cybersecurity Framework 2.0." 8 August 2023. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf
8. U.S. Securities and Exchange Commission. "SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies." 26 July 2023. https://www.sec.gov/news/press-release/2023-139
9. Lyons, Myke. Interview. Conducted by David Shluger. 31 August 2023
10. Lamb, Leslie. Interview. Conducted by David Shluger. 30 August 2023
11. Pearlson, Keri, and Chris Hetner. "Is Your Board Prepared for New Cybersecurity Regulations?" Harvard Business Review. 11 November 2022. https://hbr.org/2022/11/is-your-board-prepared-for-new-cybersecurity-regulations

The Zurich Services Corporation
Zurich Resilience Solutions I Risk Engineering
1299 Zurich Way, Schaumburg, Illinois 60196-1056
800 982 5964 www.zurichna.com

A1-P0610090-B (11/25) P1104981