The Cyber Loop:
Managing cyber risk requires a circular strategy

2019

Empower Results®

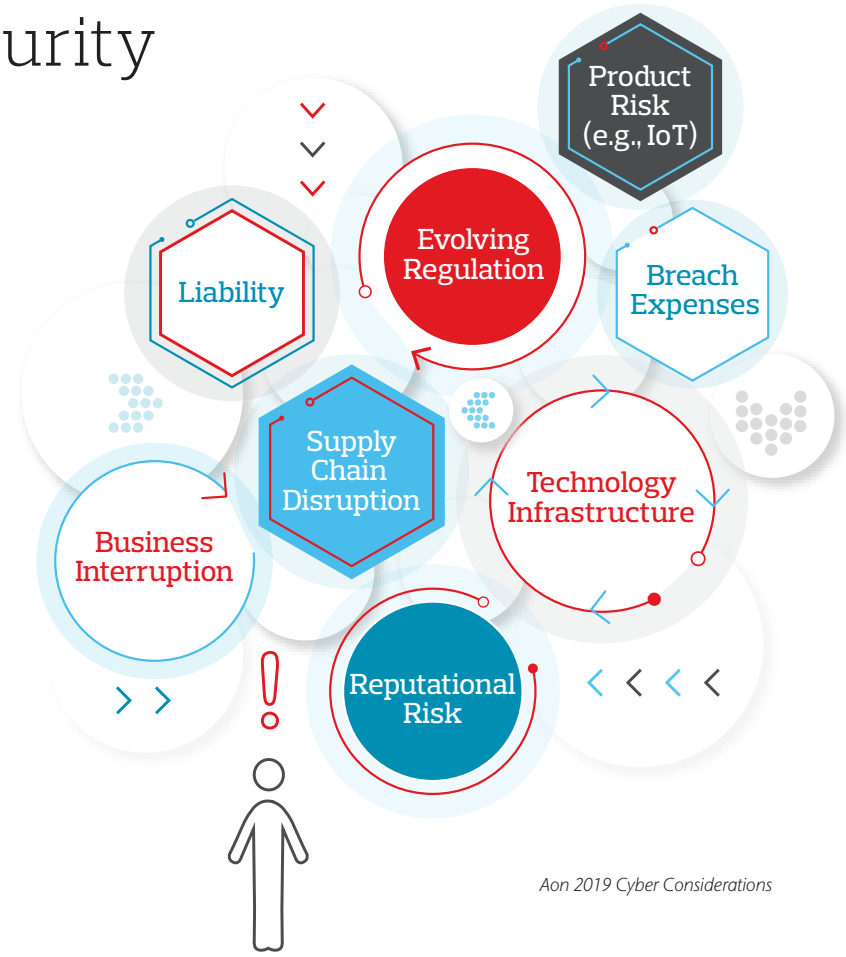
Table of Contents

There Is Nothing Linear About Cyber Security

The pressure to achieve cyber risk resilience is real. Conversations concerning resilience abound in business circles and the need to achieve a secure state is warranted when one considers that

by 2021, cyber events are expected to annually cost $6 TRILLION[i].

Companies are digitizing most of their processes; employees often operate remotely; more than 80% of U.S. companies support bring-your-own-device (BYOD) policies[ii]; and regulation is becoming ever-more complex. Cyber as a risk is felt far beyond IT and the CISO's office.



Aon 2019 Cyber Considerations

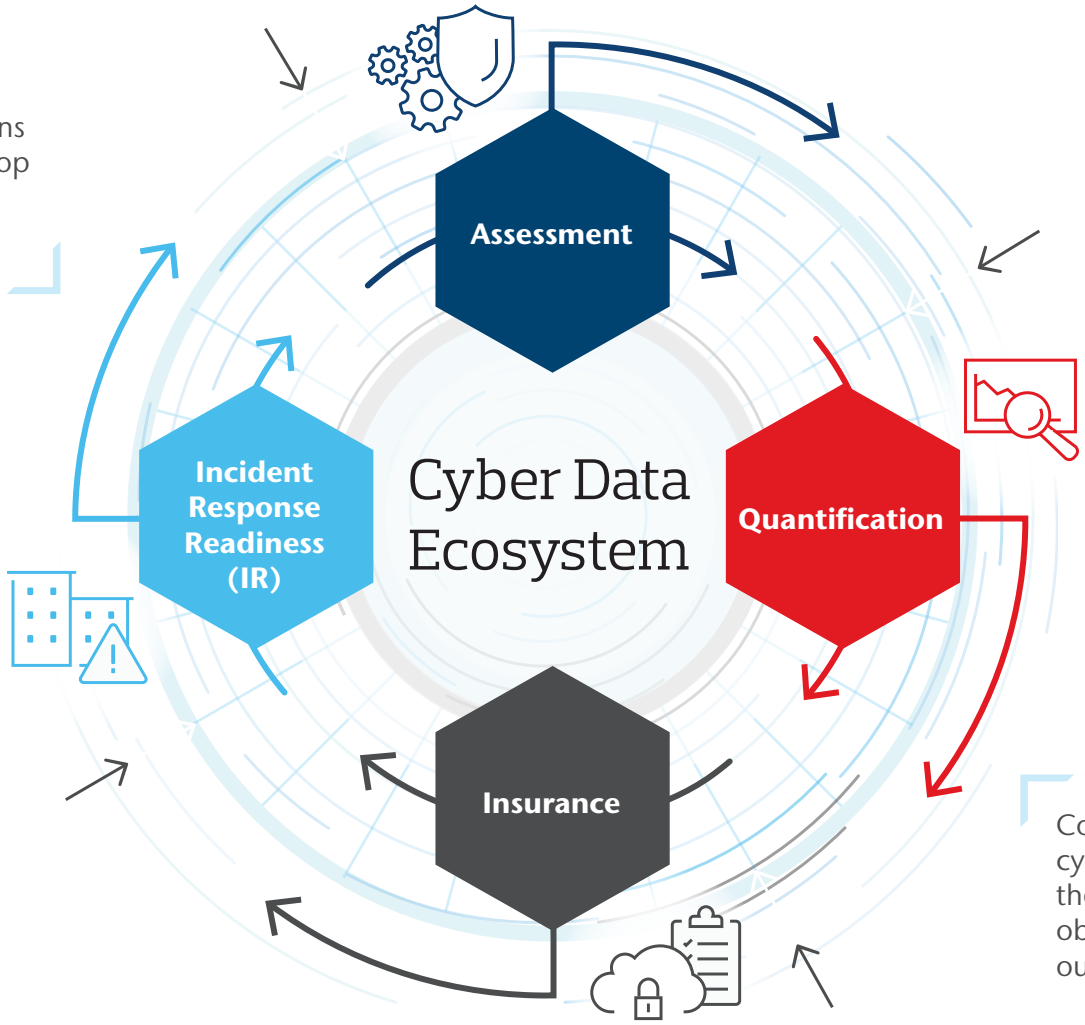
In response, the market is overflowing with technologies designed to secure organizations and operational checklists to guide companies through the landscape of resilience and remediation. But security is not achieved solely through technology, governance or compliance. Achieving resilience demands consideration of many elements and simply keeping up and staying informed about the evolving cyber risk terrain is daunting. In our **2019 Cyber Security Risk Report**, we frame our findings with the observation that the greatest challenge organizations face is simply keeping up and staying informed about the evolving cyber risk landscape. Why? Because there isn't necessarily one universal or straight-line approach to cyber security.

Each organization is unique and is at a different place in its digital journey. Thus, each organization will enter the cyber security race at a distinct point. Perhaps a significant breach demands partnering with an incident response team. Or the board calls for a strategic assessment of vulnerabilities. Successfully managing cyber risk demands that organizations persevere and embrace the dynamism of the threat. It requires an understanding of security as an iterative process. Organizations are tasked with constantly assessing and seeking actionable data about the emerging threats on the horizon. In particular, top-level management needs to understand processes around assets and vulnerabilities, balance sheet exposure, and the ability to transfer risk. Most importantly, companies must rapidly respond when an attack occurs.

It's impossible to completely eradicate cyber risk or the potential consequential damage to reputation resulting from a cyber incident. The risk is pervasive. But resilience is possible for organizations that contemplate a circular approach, which we term the Cyber Loop.

The Cyber Loop

Organizations enter the loop at different points.



Continuously cycle through the loop to obtain better outcomes.

The Cyber Loop acknowledges that each organization will start its cyber security journey from **ONE of FOUR entry points: Assessment, quantification, insurance or incident response readiness (IR).** Once in the Cyber Loop, the organization becomes an active participant in managing risk and an active participant in a greater cyber security ecosystem, engaged in continuous review, improvement and investment in cyber risk management.

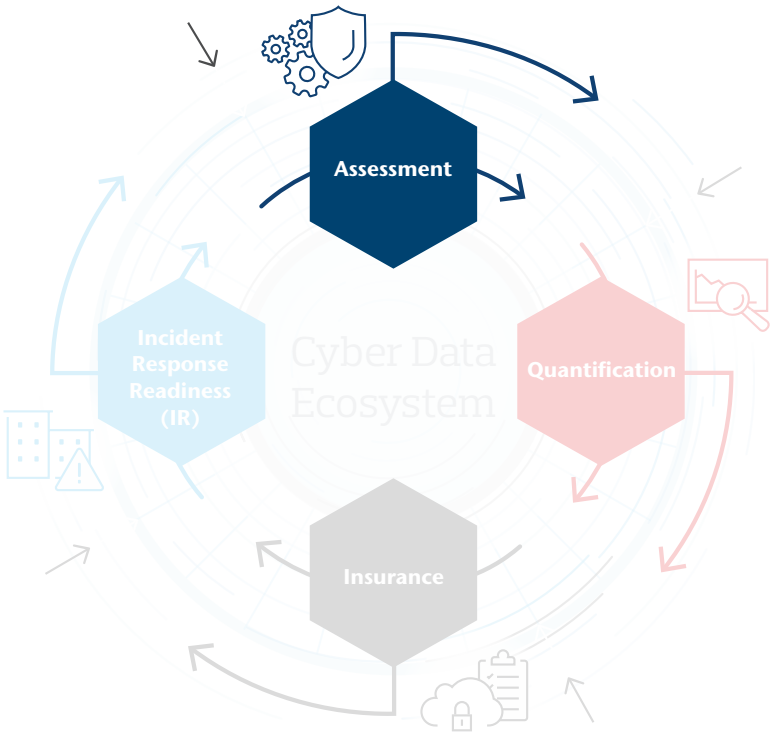
As data is collected – assessment results, quantification studies, insurance limits, peer benchmarking, claims, threat intelligence and experience garnered from actual incident response – the Cyber Loop brings everything together into one data ecosystem. With each revolution around the Loop, more data is extracted and then re-invested back into the Loop.

The result is a fresh and large pool of data related to cyber risk that can be systematically accessed to inform and improve an organization's resilience. As a company circles the Cyber Loop, it strengthens its ability to rapidly detect, respond to and recover from a cyber attack. The ability to make informed decisions gets sharper and efficiencies are created. Resilience is improved.

This approach aligns with the OODA loop, or the cycle Observe–Orient–Decide–Act, developed by the U.S. military to teach soldiers how to make decisions when there's no time to gather all the data—when agility is essential. For a company that is participating in the Cyber Loop, thinking that is fast and informed by data and experience can be engaged when – or hopefully before – a cyber event hits.

The 4 Entry Points:

Entry Point: **Assessment**



Cyber security cannot be an afterthought in any business environment. An organization that undertakes an assessment project is ready to seek the answers to some very hard questions:

- What are the most important assets we need to protect and the most likely threats we're going to face?
- What is the state of our security and controls?
- How do our people currently use our technology and data?
- How well do our people understand and comply with existing policies and procedures?
- How do we balance business needs with cyber risks?
- Can we demonstrate to shareholders, regulators and legal bodies that we exercised due diligence in securing our cyber resilience posture?
- How well are we communicating across the organization regarding cyber risk, mitigation activities and incident occurrence and response?
- Where should our budget be spent?

During an assessment, large amounts of data and insight are collected and analyzed within the ecosystem of the Cyber Loop. Critical assets, systems and operations are identified. Policies and procedures are evaluated. User behavior is confirmed. Vulnerabilities are diagnosed and prioritized, cyber security controls are benchmarked against specific threats and governance and response readiness are assessed. Through an assessment, remediation is essentially verified. Armed with this insight, leaders can make sound decisions and strategically manage the organization's cyber risk through a combination of **four paths:** *Avoid the risk, mitigate the risk, accept the risk or transfer the risk.*

1 Avoid the Risk.

Choose to not take the action that introduces the risk.

2 Mitigate the Risk.

Assess and test the risk, and put compensating controls, technologies, processes and governance in place to reduce exposure, while working to minimize impact on the business growth strategy.

3 Accept the Risk.

Assess the risk, and choose to accept the risk as is, if mitigation reduces the business benefit the organization set out to achieve.

4 Transfer the Risk.

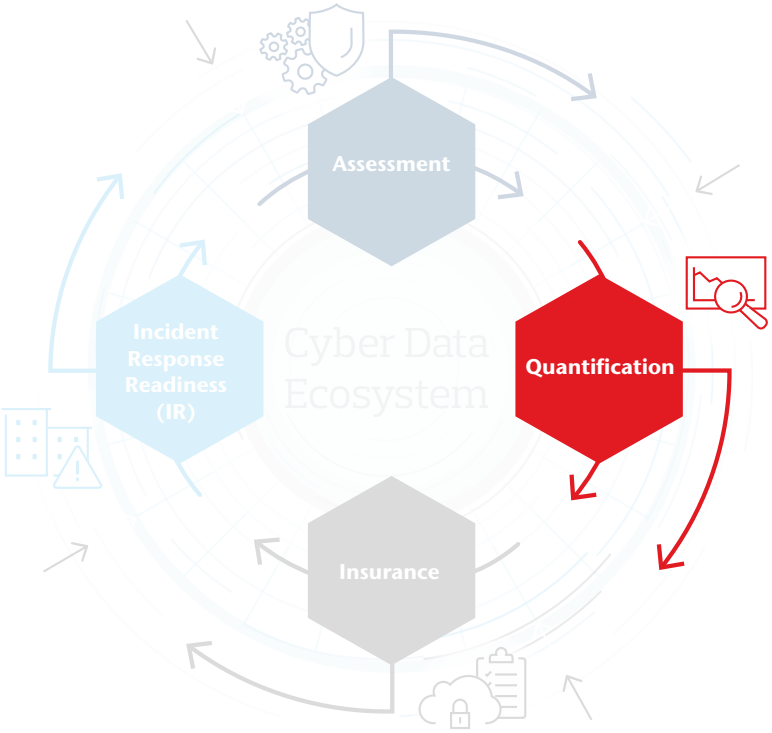
Seek cyber insurance policies to move the risk off the balance sheet.

The results of an assessment allow for strategic decisions to be made in the context of an organization's culture and risk tolerance. Security programs may be aligned with threats and corporate priorities. The organization's risk appetite is better understood. The risk manager, who has overall accountability for risk transfer, is asked to align with information technology, security, the C-suite, board, audit committee, legal and human resource teams. This new collaboration delivers a true enterprise approach to making decisions and maximizing cyber resilience. It clears confusion by drawing a roadmap that the executive team and board can understand.

The resulting strategic roadmap will be unique to the organization. It may include threat intelligence and analysis, vulnerability and insider threat management, network and application security, cloud security, regular testing and verification activity, training, outsourcing, policy and procedure revision/creation, or third-party risk management. At this point, companies may choose to act immediately, for example acting on a recommendation in response to a cyber risk finding resulting from an assessment. The company should verify the remediation did occur and that it was successful. Or, the company might circle to another section of the Cyber Loop. For example, conduct further quantification measures to put a dollar figure to critical risks or embark upon incident response planning to help reach the point of breach response readiness. Regardless of the action chosen to take post-assessment, new data is now part of the Cyber Loop ecosystem and the company's state of cyber resilience and preparedness is enhanced.

The 4 Entry Points:

Entry Point: **Quantification**



The economic losses from cyber crime – including but not limited to data breaches, network intrusions, cyber business interruptions and recent ransomware losses – now total in the billions.[iii] If something goes wrong and an organization suffers a cyber event, it may lead to significant operational, financial and reputational impact. However, many leadership teams do not know the type or materiality of these potential losses. Lacking the data and tools to better anticipate these losses, top managers who want to safeguard the balance sheet are making cyber risk investment decisions in the dark.

The process for evaluating appropriate property and business interruption insurance limits is well established, utilizing standard risk techniques that employ decades of claims data. However, the application of similarly sophisticated risk modelling for cyber risk has not widely enjoyed this technical approach. Companies have struggled to evaluate the value of stand-alone cyber insurance without an accurate measure of the financial exposure associated with the cyber threat or the likelihood of risk occurrence. As a result, companies have opted for use of insurance limit peer benchmarking and management intuition to determine the appropriate cyber insurance limits and coverage.

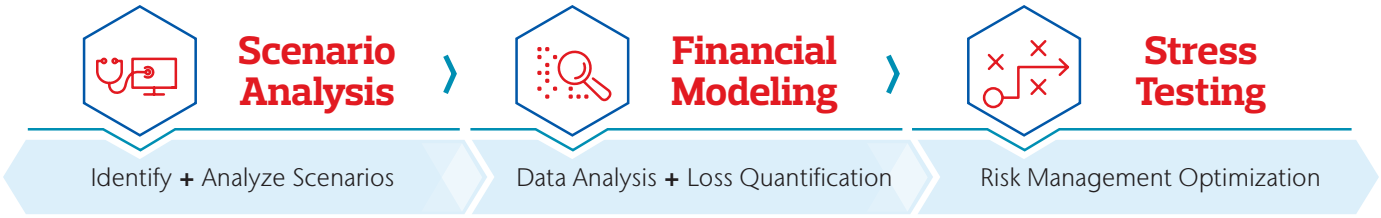
Quantification of cyber risk is critical. It uses financial modeling to help companies make smart, data-driven choices on cyber security risk management with the goal of helping safeguard the balance sheet and optimizing total cost of risk.

In a quantification study, tailored scenarios are built to understand the commercial impact of a cyber incident. This involves locating business-critical technology assets throughout the business value chain, including key suppliers and IT vendors.

Financial models using proprietary and leading data analytics are built for all identified cyber risk scenarios, effectively translating these scenarios into financial statement impact. Finally, a quantification study will stress test a company's insurance strategy and security investment roadmap.

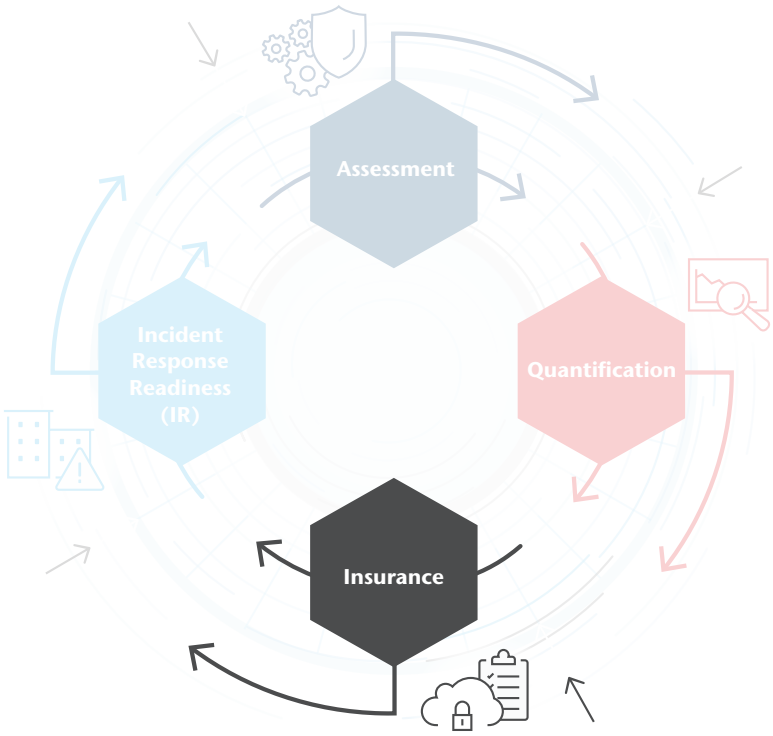
Next, an insurability analysis may determine risks that are potentially insurable, and those that are uninsurable and retained. Through this analysis, companies can measure the effectiveness of current risk management and insurance arrangements in terms of total cost of risk, as well as improve decision-making on effective uses of budget dollars to enhance cyber resilience.

By quantifying cyber risk, balance sheet impact is more clearly defined and companies can more deliberately invest in information security, business continuity programs, risk transfer strategies and cyber insurance. Should a cyber incident occur, having a quantifiable model demonstrates to key regulators and stakeholders that a thoughtful approach was undertaken and reasonable efforts were made to protect stakeholders: financial, customers, community and suppliers. **Modelling is best incorporated into an ongoing and iterative enterprise cyber security strategy and adds significant value when the impact analysis informs other activities within the Cyber Loop.**



The 4 Entry Points:

Entry Point: **Insurance**



Cyber risk goes well beyond a data breach. A significant incident can result in business interruption, impact to the supply chain and even physical injury. **The climate is becoming increasingly regulated and punitive yet cyber risk is still underappreciated as an insurable risk.**

While business disruption causes more than **double the impact to information assets than to property, plant and equipment (PP&E), companies insure PP&E to a greater degree (60%) than information assets (16%), and only 28%** of companies surveyed by the Ponemon Institute in **2019 purchase cyber insurance.**[iv]

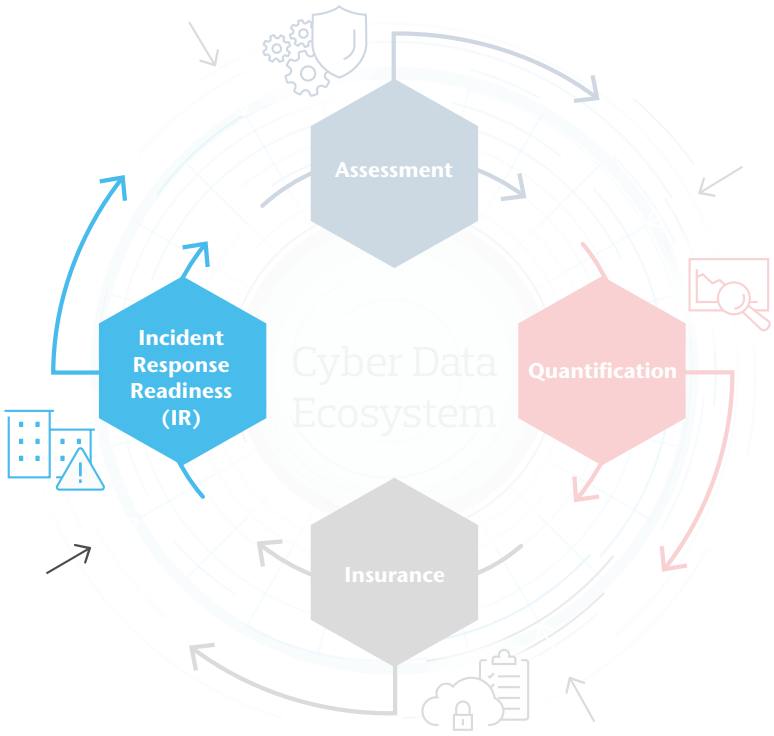
Managing cyber as an enterprise risk necessitates that a company asks: Does our organization have an effective strategy, reflective of exposures, including third-party exposures, to mitigate potential financial losses? This requires disparate stakeholders to connect; to address the risk in unison, including but certainly not limited to the CIO, CISO, head of disaster recovery, general counsel, treasurer, risk manager and human resources manager. If approached from this holistic, enterprise view, the cyber insurance and risk transfer process can serve as the bowtie to pull key stakeholders together. Increasingly, cyber insurance is being required by contract and is demonstrative to clients and vendors that a company has contemplated multiple aspects of cyber risk across the enterprise and has invested in balance sheet protection. As coverage continues to evolve, it is becoming more valuable for companies. According to Aon data, over 75 insurers provide over $1B in cyber insurance capacity across North America, London, Europe, Bermuda and Asia. This growing number of insurers has helped develop appetites for large, complex risks.

Once engaged in this phase of cyber resilience preparation, companies will find more than one way to transfer and manage quantified cyber risk. Perhaps it does make sense to transfer a portion to the cyber insurance market, but maybe an alternative risk retention, or self-insurance financing strategy, is warranted. **The more data a company has acquired by revolving around the Cyber Loop, the more visibility it has to help make sound risk management decisions to help protect the organization against financial loss.**

Global cyber insurance premiums expected to grow from **$4B in 2018 to $20B by 2025.**[v]

The 4 Entry Points:

Entry Point:
Incident Response Readiness (IR)



A company receives a call from the FBI saying that sensitive data is being leaked; a ransomware message flashes threatening business interruption, or shutdown, due to the inability to access critical data if demands are not met; or, maybe a credit card company sends notification that the company's point of service (POS) system is suspected for PCI compromise, serving as the source of an attack on card holders.

Every minute of an undiscovered, unaddressed or uncontained breach costs your company in terms of reputation and monetary damages.

Entering the Cyber Loop at incident response readiness (IR) can be proactive, for example developing a response plan and conducting tabletop exercises in preparation for a likely attack; or reactive, when faced with an urgent need to find, contain and mitigate an incident. For an organization that has been managing cyber risk with a circular strategy, significant value is unlocked during incident response readiness. Those that have completed assessment work will be familiar with the environment from a network topography standpoint and will know the location and type of critical data. There will be an understanding of policy, procedure and people. Armed with this knowledge, responders can more quickly develop a picture of what is going on, and how to shut down the compromise. Once in the Cyber Loop, companies receive immediate access to real-time attack data and indicators of compromise (IOC), making it faster to trace an attacker's footprints and determine the nature of the attack or what information might have been impacted.

Incident response is also bolstered through preparation. Preparation can be the difference between a company that is ravaged by an attack, and one that finds it a disruption. A company with an interdisciplinary leadership team that has practiced response to common scenarios like trade secret theft, credit card data breach, healthcare data breach (PHI), personally identifiable information (PII) breach, wire fraud, business email compromise (BEC), ransomware incident, hacktivist attack and other foreseen attacks, is likely to make good decisions at the 11th hour and reduce the risk for the balance sheet and stakeholders.

Realizing the Full Potential of the Cyber Loop
Case Studies

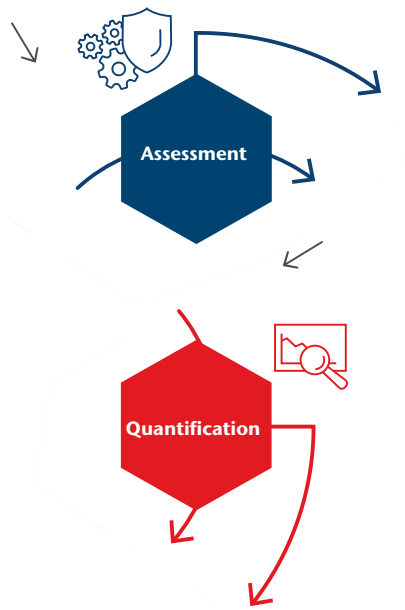
Every organization can strengthen its posture when cyber risk is managed with a circular and holistic strategy. Below are engagement examples that illustrate the value of operating within the Cyber Loop. Each company enters the Cyber Loop at a distinct point and each employs a circular strategy to achieve resilience.

THIS FINANCIAL INSTITUTION WANTED A FULL SUITE OF CYBER SECURITY RISK SERVICES

ENTRY POINT: Assessment and Quantification

A financial institution in Europe was interested in purchasing cyber insurance for the first time. However, this is not where they entered the Cyber Loop. Through the tender process, it became clear that the organization desired one consultant to help address cyber security risk issues on a holistic basis, including risk assessment, quantification, incident response and claims reporting. Our team started with an assessment and quantification study, developing customized loss scenarios to determine the potential financial loss the institution faced. Once complete, the organization was able to confidently select the limit of liability for their cyber insurance purchase. Additionally, they selected several proactive strategies to help improve their overall cyber security posture, as well as test their incident response plan, including penetration testing, red teaming and a table top exercise. Lastly, it was important to this financial institution that incident response was seamless, in terms of engaging with an incident response team that could also facilitate claims reporting to its cyber insurance carriers.

END RESULT: Overall improved cyber security posture via a full revolution of the Cyber Loop.



THIS MUNICIPALITY SUFFERED AN IMMENSE MALWARE ATTACK

ENTRY POINT: Incident Response Readiness (IR)

A municipality suffered from an immense malware attack, resulting in more than 20 gigabytes of personal data being sent to an unknown site. Leadership had been contemplating a cyber insurance program before the attack but was still reviewing the added value when an attack occurred. Once the crisis was over and the breach was contained, we performed a cyber risk assessment to identify critical assets and vulnerabilities, and to help mitigate a future attack. We also conducted crisis management simulation training and tabletops to prepare the municipality for rapid, on-the-ground response. Now ready to gain more visibility and dig deeper, the municipality circled the Loop to quantification. We performed cyber impact analysis and financial modeling, providing leadership with the data required to confidently make decisions about what risks to maintain, mitigate or transfer. The circular approach then moved to insurance, where we helped to not only secure coverage but also advised on policy wording that reflected the municipality's cyber risk and was in step with their risk tolerance level.

End result: Empowered a security culture and helped improve resilience for this municipality.

Realizing the Full Potential of the Cyber Loop (continued)

Case Studies

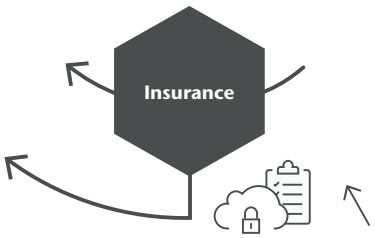
THIS LIFE SCIENCES COMPANY SOUGHT OPTIMAL CYBER INSURANCE STRATEGY

ENTRY POINT: Insurance

Exposure to cyber risk weighed heavily on the minds of the security managers at a large pharmaceutical organization. Operating worldwide with a complex network topology, the organization found it difficult to centralize the information security control documentation that would be necessary to present the risk to the insurance market. Leadership was also unable to quantify their cyber exposures and did not have an appropriate indicator of the required level of coverage. Working with senior leaders in the security function (CISO), technology group and treasury, we recommended a top-down scenario analysis workshop to establish the priority risks facing mission-critical technology assets across the business. Scenarios were built out in great technical detail and involved analysis of internal data sets on critical system dependencies, network topography, data mapping exercises, internal tactical and operational threat intelligence and post-activity reports from previous critical incidents. Three critical scenarios were identified: Pharmacovigilance data breach, operational technology (OT) production system downtime and critical vendor failure.

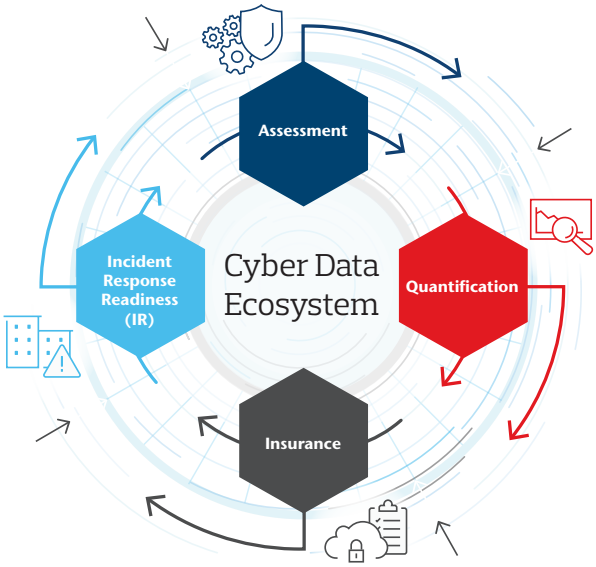
Based on this assessment, the company circled the Cyber Loop to quantification and developed a financial impact model that put numbers to the loss exposure and aligned the insurable risk exposures with an optimized insurance strategy. By involving all stakeholders, a clear line of sight to cyber exposures across the enterprise was established, helping to secure best-in-class insurance coverage.

End result: For the first time, the board was able to sanction a capital expenditure for the procurement of cyber insurance.



Evolution Demands Revolution: Realizing the Full Potential of the Cyber Loop

The Cyber Loop calls for companies to actively participate in managing cyber risk in a greater cyber security data ecosystem. There is no magic bullet or linear approach to cyber security. Managing cyber as an enterprise risk requires continuous review, improvement and investment in cyber risk management. **Assessment, quantification, insurance and incident response readiness are four distinct yet interconnected entry points for managing the risk.** When operating with a data mindset and a circular strategy, a company can effectively strengthen its posture and help develop cyber risk resilience.



Contributors

Jordan Kendall
Chief Operating Officer
jordan.kendall@aon.com
+ 1 212.981.2672

Stephanie Snyder
Commercial Strategy Leader
stephanie.snyder@aon.com
+1 312.381.5078

Thomas E. Abel
Senior Vice President of Marketing and Business Development
thomas.abel@aon com
+1 212.903.2818

Adam Peckman
Practice Leader – Cyber Risk
adam.peckman@aon.com
+1 201 856 9364

Chad Pinson
Executive Vice President Engagement Management — Cyber Security
chad.pinson@aon.com
+1 214.377.4553

Contacts

Jason J. Hogg
Chief Executive Officer
jason.j.hogg@aon.com

Eric Friedberg
Co-President
eric.friedberg@aon.com
+1 212.981.6536

Edward Stroz
Co-President
edward.stroz2@aon.com
+1 212.981.6541

Americas

Christian E. Hoffman
President
christian.hoffman@aon.com
+1 212.441.2263

CJ Dietzman
Security Advisory Practice Leader
cj.dietzman@aon.com
+ 1 212.903.2828

Jay Stampfl
National Sales Leader — Cyber Security
jay.stampfl@aon.com
+1 203.682.6470

EMEA

Onno Janssen
Chief Executive Officer
onno.janssen@aon.com
+49 (4) 03.605.3608

Vanessa Leemans
Chief Commercial Officer
vanessa.leemans@aon.co.uk
+44 (0) 20.7086.4465

References

i. Cisco/Cybersecurity Ventures 2019 Cybersecurity Almanac, 02/06/19.

ii. Syntonic 2016 Report, BYOD Usage in the Enterprise

iii. Centre for Strategic & International Studies, 02/21/2018

iv. Ponemon 2019 Intangible Asset Financial Statement Impact Comparison Report, 05/01/2019.

v. Allianz S.E., 01/16/2018.

Empower Results®

About Cyber Solutions

Aon's Cyber Solutions offers holistic cyber risk management, unsurpassed investigative skills and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets and recover from cyber incidents.

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

Visit aon.com/cyber-solutions for more information.

Empower Results®