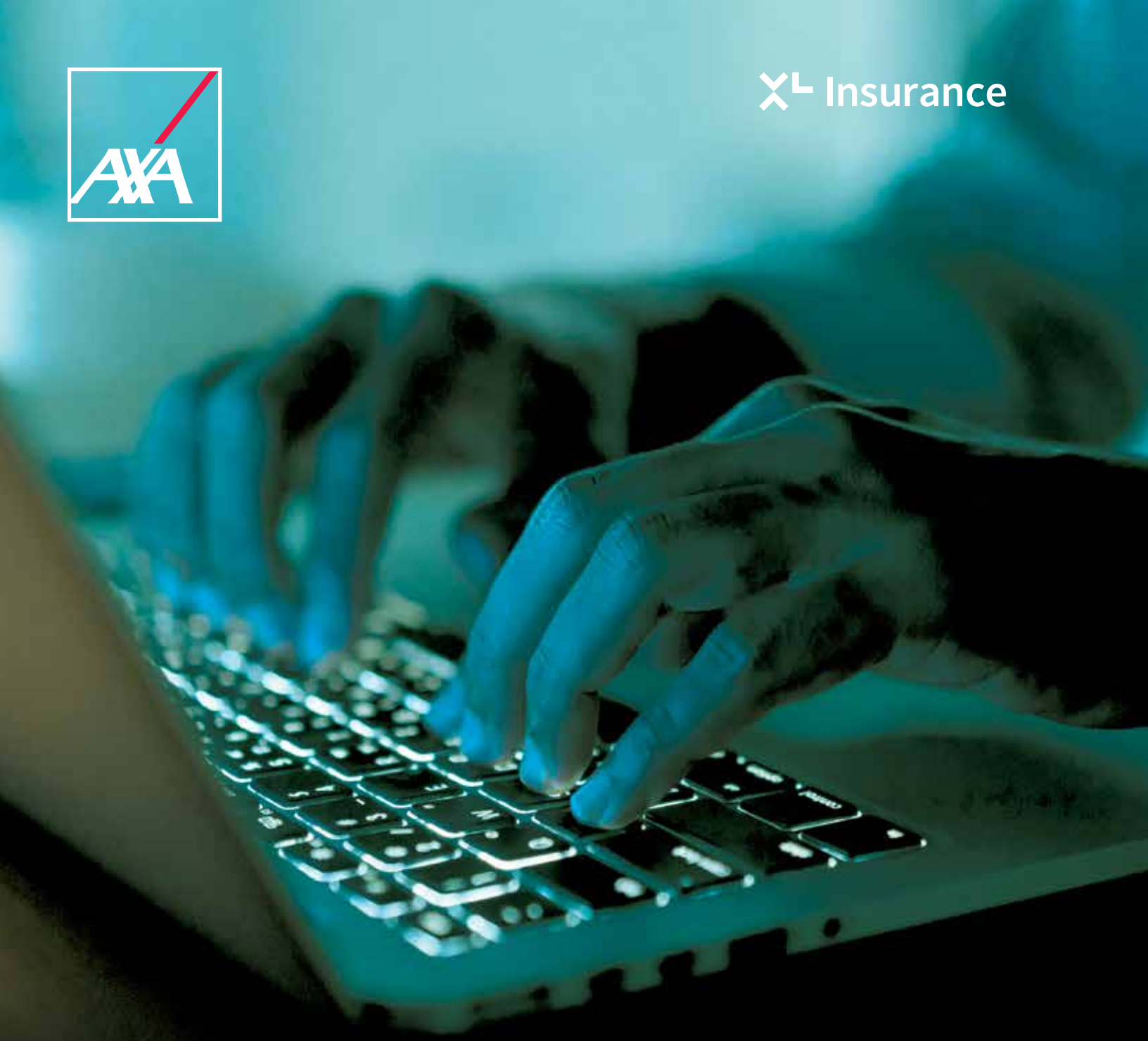


AXA

XL Insurance

Tailoring cyber risk assessments to fit your organization

Best practices to keep your business moving forward

co-authored by

S-RM

Ten years ago, cyber attacks were not considered a top enterprise risk.

Today, they are ranked the 5th most likely global risk and 7th most impactful one, according to the World Economic Forum Global Risk Perception Survey 2018-2019.[1] As the risk of cyber incidents grows, so does the number of organizations realizing the importance of having a cybersecurity program in place to protect them. Cyber risk assessments can form the foundation of an effective cybersecurity program. This article outlines the varying strategies used in conducting cyber risk assessments and the steps to get the most out of the process.

2
Benefits of cyber risk assessments
Existing frameworks

5
A tailored approach is best
Preparing for an assessment

6
Conducting the assessment

10
Communicating the results
Maintaining the risk assessment

11
Conclusion
Key takeaways

12
Sources

Benefits of cyber risk assessments

The National Institute of Standards and Technology ("NIST") defines a risk assessment as "the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation, resulting from the operation of an information system." [2] More simply, the purpose of a risk assessment is to inform organizations of where they are most at risk so they can decide the most effective and efficient ways to manage cyber risk.

Cyber risk assessments provide a prioritized list of cyber risks based on their potential impact. This allows organizations to focus their response. In today's complex business environment, every assessment is unique. Businesses that do not conduct cyber risk assessments are leaving themselves underinformed about their cyber risk exposure, which can lead to blind spots and breaches. Cyber risk assessments also:

- Inform decision makers of where the organization is most at risk, allowing them to prioritize resources when most do not have the budget to fully manage all their risks. The Ernst & Young Global Information Security Survey 2018-19 found that 87% of organizations do not yet have sufficient budget to support desired levels of cybersecurity. [3]
- Support compliance with regulatory requirements as cyber risk assessments are increasingly becoming a regulatory expectation. [4]
- Inform decision makers of how to manage risks, whether that be to mitigate, accept, avoid or transfer (for example, insure) them.
- Facilitate decisions that reduce long-term costs. Although conducting the initial risk assessment can be time consuming, and managing risks involves additional expense, identifying risks and managing them effectively should save money in the long run.

The benefits that risk assessments create for organizations are clear. Most organizations should conduct cyber risk assessments; even small companies can have significant cyber risks. For example, art collectors often have a small staff but should understand how they are protecting their business from the risk of large fraudulent fund transfers, which have the potential to bankrupt their company.

Existing frameworks

There are numerous frameworks and standards available to help understand and plan a risk assessment process; however, they are all based on the following concepts:

- Risk is a function of the likelihood that a threat will occur and the impact that it would have if it did.
- The vulnerability present in the environment influences risk likelihood (for example the more vulnerable you are, the more likely you are to experience a cyber breach), as does the attractiveness of the target (for example the value of the data you hold, the perceived value of disruption, etc.)
- When mitigating risks, it is not possible to reduce risk to zero; there will always be residual risk. The goal is to be aware of and comfortable with the amount of residual risk, which is often referred to as "risk tolerance".

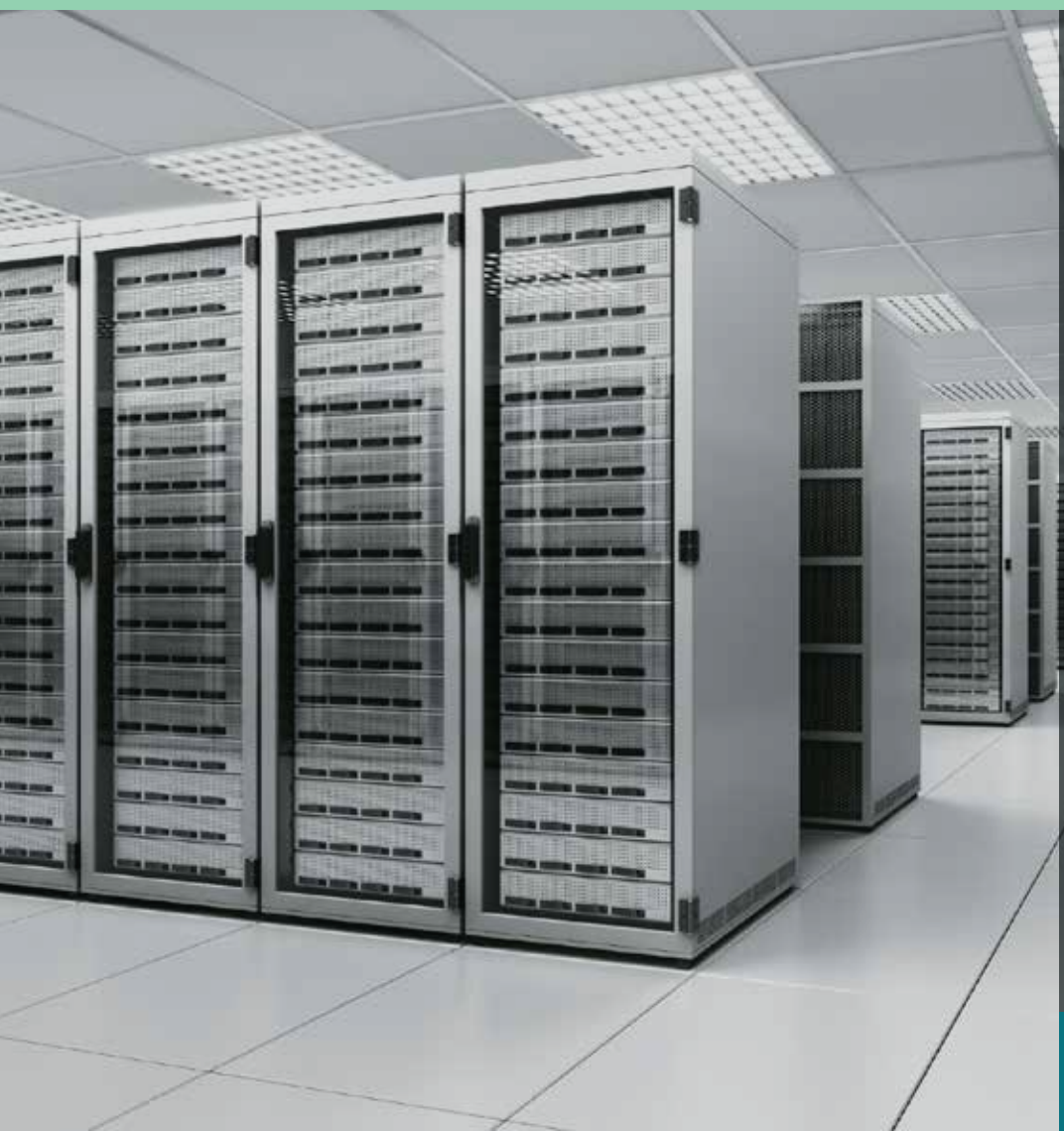
The process should be continuous as risks and business environments change regularly. Best practice is to update risk assessments whenever there is a significant business change or yearly, whichever comes first.

Popular cyber risk assessment frameworks include: ISO/IEC 27005 [5], NIST SP 800-30/39 [6], Octave Allegro [7], Factor Analysis of Information Risk ("FAIR") [8], Control Objectives for Information and Related Technology ("COBIT") [9], as well as many more. The following ISO and NIST frameworks are some of the most popular:

- **ISO/IEC 27005:** This standard provides guidelines for information security risk assessments and is designed to assist the satisfactory implementation of a risk-based information security program. [5] It covers people, processes and technology. ISO standards are internationally recognized and designed to be widely applicable across organization types; however, they can lack a prescribed structure, and some find them nebulous, especially for small and medium sized enterprises (SMEs).
- **NIST SP 800-30/39:** This framework contains a clear set of guiding steps to support the risk assessment and risk management process. It is primarily focused on technical risk management for IT systems and benefits from a clear prescriptive approach. [6]

For SMEs and others that are new to the risk assessment process and have limited resources to work with, it may be useful to implement software that streamlines the process with pre-defined threats and vulnerabilities. Ideally, an experienced cyber risk assessor should recommend the most effective approach and perform the assessment.

Businesses that do not conduct cyber risk assessments are leaving themselves underinformed about their cyber risk exposure, which can lead to blind spots and breaches.



The Ernst & Young Global Information Security Survey 2018-19 found that

87%

of organizations do not yet have sufficient budget to support desired levels of cybersecurity. [3]

Research conductd by NTT found that

43%

of businesses believe that cybersecurity is purely an IT function. [10]

A tailored approach is best

Despite their clear importance, many organizations don't conduct cyber risk assessments because of the perception that it is a complex process that provides little value. Many will instead simply implement common security controls in response to the risks they read or hear about. However, this typically leaves businesses exposed, with an unbalanced security program focused on the wrong priorities.

Although the voluminous cyber risk assessment standards and frameworks can be dizzying, they're beneficial as guidelines to form a simple starting point. Organizations can create an approach that is feasible for them, basing the approach on their structure, culture and risk profile. NIST 800-30, for example, includes simple risk assessment templates in the appendices of the publication.[6] There are four general steps that are consistent throughout any risk assessment, irrespective of the framework adopted: preparation, assessment, communication and maintenance.

Preparing for an assessment

To prepare for the assessment, organizations should consider the following aspects:

Purpose
It must be clear why the organization is conducting a risk assessment because the context will determine which types of risks to consider and the specific impacts they could have on the organization. For example, is the purpose to protect reputation, comply with regulatory requirements, comply with contractual obligations, pass an audit for SOC, ISO 27001, or other purposes?

Scope
The scope should clearly define what is included in the assessment and what is excluded. Proper scoping will decrease ambiguity and can help to keep the assessment on track and within budget.
The scope should also consider what the outputs should inform. For example, are the results of the risk assessment informing the following year's security budget?

Roles and responsibilities
Although the risk assessment process may be managed by a group of people, it should be owned by a single individual in order to enforce proper accountability. Regulators are increasingly holding organizations liable for cyber breaches and are looking to those who are responsible for managing an organization's cyber risk. Research conducted by NTT found that 43% of businesses believe that cybersecurity is purely an IT function.[10] Due to the fact that cyber incidents affect the whole business, and not just the IT department, an effective risk assessment should be the responsibility of senior leadership.

Conducting the assessment

The process of conducting a cyber risk assessment varies slightly between the different frameworks; however, it can be broadly summarized into the following four actions.

1

Identifying risks

Risks represent the extent to which an entity is threatened by an event occurring.[6] A risk can be defined as the potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability. Before organizations can analyze their risks, they must identify:

- **Assets:** anything of value that needs to be protected. For cyber risk assessments, this usually includes data, but can also include reputation and people.
- **Threats:** anything that could negatively impact the confidentiality, integrity or availability of assets.
- **Vulnerabilities:** security weaknesses that can be exploited by threats.

Once organizations have identified their assets, threats and vulnerabilities, they can analyze their risks.

2

Assessing risks

Risk is assessed by determining the likelihood that an incident will occur and the impact that it would have. The likelihood estimates the probability and frequency of it occurring. This is dependent on both the vulnerability and attractiveness of the asset in question and the presence and capability of threat actors. Assets that have many vulnerabilities could be a likely target for attackers as they may be easy to exploit. Furthermore, assets without the necessary security in place could be compromised accidentally by a negligent insider. The attractiveness of the target will also factor into the risk. Assets that hold a vast amount of data, or assets that could yield a substantial profit for the attacker could also be frequently targeted since the possible return of a successful attack is high.

The impact component estimates the level of harm that could occur. When assessing impact, companies should consider the confidentiality, integrity and availability (commonly known as CIA) of the asset and then determine the consequences if it were to become compromised. The importance of these different attributes will vary widely between businesses and individual assets.

Sometimes loss of revenue due to business interruption outweighs direct financial losses when funds are redirected or stolen.

The following impact categories are commonly used:

Financial

Most companies are primarily motivated by profit, therefore there is often a large emphasis on financial impact. However, other scenarios, such as those listed below, can have an indirect financial impact and capturing these overlapping impacts can prove challenging. Sometimes loss of revenue due to business interruption outweighs direct financial losses when funds are redirected or stolen. For example, following the 2017 Petya outbreak, FedEx reported that it lost revenue due to decreased volumes at TNT Express and incurred incremental costs from contingency plans and remediation of affected systems. The financial impact in this case was approximately $300 M.[11]

Reputational

Cyber incidents can also erode reputations, thereby damaging the customer's trust in the organization and their willingness to continue supporting it. This can lead to a loss of customers and revenue, which can then result in a reduction in profits. For example, in 2015, TalkTalk, a British telecom company, experienced a data breach that exposed personal details of nearly 157,000 customers.[12] The details included full names, mailing addresses, email addresses, dates of birth, TalkTalk customer numbers, mobile numbers and bank details.[12] TalkTalk's reputation was severely damaged and resulted in a loss of 101,000 customers.[13]

Legal/Regulatory

Data protection laws are becoming increasingly sophisticated as the world becomes more digitized. If an organization fails to protect the personal information it holds, it may face fines and regulatory actions. In July 2019, British Airways was fined £183 million by the Information Commissioner's Office ("ICO") following a breach of its security systems. The breach exposed sensitive data of approximately 500,000 people.[14] According to the ICO, the incident involved user traffic to the British Airways website being diverted to a fraudulent website.[15]

Assessing risks (continued)

A key challenge is how organizations choose to present this information using either a quantitative or qualitative method. The qualitative approach associates well-defined definitions with certain thresholds, such as “Low,” “Medium,” and “High.” These thresholds can be associated with numerical values if they are easier to visualize or needed for use in equations. A quantitative method uses numerical information to define thresholds and is usually based on factual and measurable data to calculate likelihood and impact; this method is commonly used to expresses risk in monetary terms. Each method has its own advantages, so organizations must determine which of these methods would be most appropriate for them. Typically, it is easier to use a qualitative method, especially if this is the first time a risk assessment has been performed.

QUALITATIVE	
Strengths	**Weaknesses**
Easier to comprehend for a wider audience	Often argued to be too subjective as it is based on the opinion of the analyst conducting the assessment
Generally faster to perform as less research is needed	Can be inconsistent

QUANTITATIVE	
Strengths	**Weaknesses**
Considered more thorough than the qualitative method	Time consuming/expensive
Risk is explained in monetary terms, which can easily be translated into the company’s wider agenda	Can be considered too technical
Accurate and consistent	Data can be hard to find or may not exist

There is an opportunity to use a hybrid approach that leverages the advantages afforded by both methods. For example, the qualitative approach could be used to quickly capture the relevant impact and likelihood descriptions, highlighting the most critical risks, and then on a second pass, replace the qualitative descriptions for the most significant risks with quantitative results. This way, time isn’t wasted on using the lengthier quantitative approach for insignificant risks. The additional effort spent to generate quantitative results improves the effectiveness of the reporting to senior management. It can make it easier to budget for risk treatment options when the cost-benefit analysis becomes much clearer.

3

Identifying mitigation measures

After risks are identified and assessed, decisions should be made to manage, or treat, the risk. Typically risk mitigation is considered first to understand what resources would be needed to reduce the likelihood and/or impact of a risk, but sometimes it is abundantly clear that a different risk treatment option is a better choice (these are covered in the next step). The decision to mitigate the risk is a balance of the following types of mitigation measures:

- **Prevention:** Measures that reduce the likelihood of a risk materializing
- **Detection:** Measures that alert an organization when there has been a possible cyber incident, with the goal of reducing the impact of the incident
- **Recovery:** Most commonly associated with implementing a backup regime so that, in the event of a cyber incident, lost data can be recovered, also with the goal of reducing the impact of an incident that's already occurred.

There is often a misconception that this step requires a large technology investment, which is a key challenge for many organizations. However, while technology can be required to mitigate some risks, governance via implementation of policies, procedures and training plays a key role in mitigating risk. This can also provide a low-cost solution for organizations that do not have a large budget for information security. However, stronger governance solutions usually require more time, rather than direct spend, to be effective.

Generally, organizations that can demonstrate strong cyber hygiene will also receive the most competitive cyber insurance premiums and terms.

4

Addressing residual risk

In the modern business environment, it is impossible to completely mitigate risk. Therefore, organizations need to decide what level of risk they are willing to tolerate. For risk that exceeds the tolerable level, organizations should decide what to do with it. After mitigating risks, there are three remaining risk treatment options:

- **Avoid:** Avoiding a risk occurs when the organization ceases the activities that create the risk. This often happens when a company is unwilling to accept residual risk but is also unwilling to spend on reducing it, or when an organization is not able to reduce the risk to an acceptable level.
- **Accept:** When management accepts a risk, they decide to take no further action to manage it even though it is above the tolerable level. This is common when the cost of the other risk treatment options outweighs the cost of the risk materializing.
- **Transfer/insure:** Risks can be transferred in a variety of ways, but typically they are insured or otherwise shared amongst others. Cyber insurance is ideally reserved to treat low likelihood, high impact events. As the potential impacts of cyber incidents are becoming increasingly catastrophic and unpredictable, decision makers are turning their attention to cyber insurance as an attractive option, because it can be obtained without disrupting operations.

It is not uncommon to use a few treatment options for the same risk. For example, the risk of ransomware infection could be mitigated with good patching and next-gen malware protection, insured via cyber insurance, and any remaining, or residual risk, accepted by management.

Using the previous example of the FedEx data breach, it has been revealed that FedEx did not have insurance to help cover the cost of the cyber attack. After the incident, FedEx revealed they were considering cyber insurance options.[16] However, it should be noted that cyber insurance does not replace thoughtful risk management. Although insurance is a very useful risk treatment option, it is prudent to avoid a breach altogether. Some tangible and intangible breach-related costs can't be insured, not least of which is the stress it puts on the employees. Generally, organizations that can demonstrate strong cyber hygiene will also receive the most competitive cyber insurance premiums and terms.[17]

Communicating the results

Often, risk assessments are performed by stakeholders that might not have significant influence over budgeting. Therefore, it is vitally important that senior leadership is informed of the results. Sometimes there is a perception that communicating the results won't have a positive impact on future risk management efforts, but in the current risk and regulatory environment, senior management has a duty to protect their organization from cyber attacks.

The main challenge with this step is ensuring that the data is framed appropriately for the audience so that it is well understood and decisions can be made. A survey conducted by McKinsey & Company found that 54% of executives said that risk reports are too technical.[18] For example, board members may wish for the information to be presented in quantitative financial terms to enhance their decision-making processes, especially when cyber risks are compared to other enterprise risks that also need to be considered. Additionally, being able to instantly see a risk's monetary implications is likely to engage decision-makers. When presenting the findings back to the organization at large, it is more effective to simplify the findings so that the most relevant risks are comprehendible to the average employee at the company. Those risks that are relevant to most employees can then be included in the cybersecurity awareness and training materials that employees should receive on a periodic basis.

A survey conducted by McKinsey & Company found that

54%

of executives said that risk reports are too technical.[18]

Maintaining the risk assessment

Risk assessments are not a one-off activity. They should be updated at defined intervals or when significant changes in the organization or threat environment occur. For example, the volume of Internet of Things (IoT) devices installed from 2014 to 2018 increased by 2.63 billion across the business sector. By 2020 this is projected to grow by a further 3.39 billion.[19] This rapid integration of devices into enterprise IT systems is likely to change organizations' risk exposure and represent an opportunity to update a cyber risk assessment.

For those that currently perform risk assessments, the process is typically viewed as a compliance exercise, often occurring once per year, or less. Approaching cybersecurity as a compliance activity instead of a proactive, consistently improving program increases the chances that risks could materialize. The UK's National Cyber Security Centre refers to compliance-based risk assessments as defensive risk assessments.[20] Defensive risk assessments frequently become tick box exercises with legal motivations to avoid claims of negligence. Conducting these types of risk assessments does not produce a true and accurate picture of risk. Instead, organizations should conduct a proactive risk assessment which examines significant risk impacts in an ongoing process that constantly monitors the threat environment.

Continuous risk monitoring increasingly requires technology solutions that automate the process. Large, complex organizations will require more technology and automation in order to respond to their threat landscapes effectively. In much the same way that we are able to understand when there is an elevated risk of wildfires, we can understand when there is an elevated risk of cyber attack using technical indicators. For example, technology can tell us if there are specific vulnerabilities present in an enterprise IT environment and if there is threat intelligence that indicates that those vulnerabilities are actively being attacked.

Conclusion

The first step to managing cyber risk is to understand it, and the best way to understand it is to properly assess and document it. Given the wide range of organizational structures, motivations, resources and other intricacies, it is not possible to prescribe a given risk assessment methodology, but as explored in this paper, it is possible for any organization to perform a cyber risk assessment that is scoped appropriately using the resources available. Cyber risk assessments form the foundation of good cybersecurity programs, which is increasingly a board-level concern as the world continues to deal with constantly evolving cybersecurity threats.

Key Takeaways

1

There is not a one-size-fits-all approach to risk assessments; organizations may need to adapt existing frameworks to create an approach that is suitable for them.

2

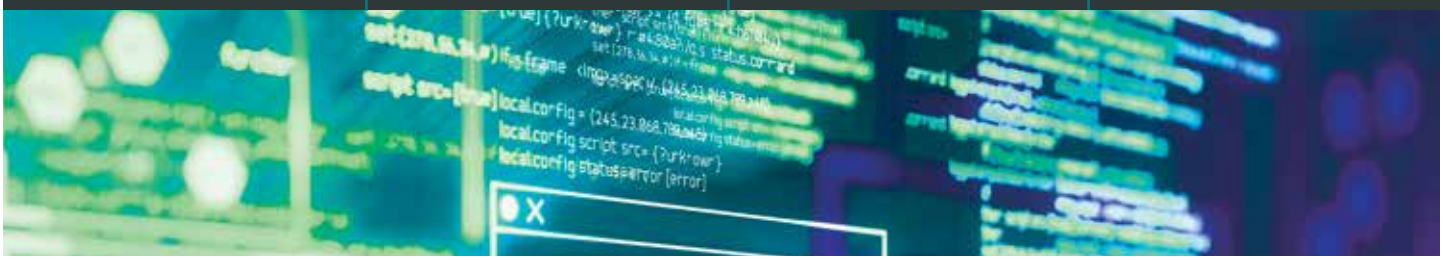
To be effective, risk assessments should be sponsored by individuals with sufficient authority.

3

The risk assessment results should be communicated to senior management in a format that is understandable in order to increase awareness and produce a tangible action plan.

4

Risk assessments are a continuous activity; cyber threats should be monitored because they continuously evolve.



Cyber risk assessments form the foundation for good cybersecurity programs, which is increasingly a board-level concern as the world continues to deal with the cybersecurity crisis we are facing today.

Sources

[1] 'The Global Risks Report 2020', World Economic Forum, 2020.

[2] 'NIST Special Publication 800-30 Managing Information Security Risk: Organization, Mission and Information System View', NIST, March 2011.

[3] 'Is cybersecurity about more than protection? EY Global Information Security Survey 2018-19', Ernst & Young, 2018.

[4] 'Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices, Financial Stability Board, 13 October 2017.

[5] 'ISO/IEC 27005: 2018 Information technology – Security techniques – Information security risk management', ISO, July 2018.

[6] 'NIST Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments', NIST, September 2012.

[7] 'Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process', Carnegie Mellon University, May 2007.

[8] FAIR Institute

[9] 'COBIT 4.1: Framework for IT Governance and Control', ISACA, 2019.

[10] 'Businesses must assign a cyber risk owner', NTT, 22 October 2018.

[11] 'NotPetya cyber attack cost TNT at least $300m', BBC News, 20 September 2017.

[12] 'TalkTalk data breach customer details found online', BBC News, 22 May 2019.

[13] 'TalkTalk loses 101,000 customers after hack', Telegraph, 2 February 2016.

[14] 'British Airways faces record £183m fine for data breach', BBC News, 8 July 2019.

[15] 'Intention to fine British Airways £183.39m under GDPR for data breach', Information Commissioner's Office, 8 July 2019.

[16] 'FedEx reconsiders cyber insurance after attack hits profit', Business Insurance, 20 September 2017.

[17] Kshetri, Nir 'The Economics of Cyber-Insurance', IEEE IT Professional, Nov/Dec 2018.

[18] 'Cyber risk measurement and the holistic cybersecurity approach', McKinsey & Company, November 2018.

[19] 'The Internet of Things (IOT)* units installed base by category from 2014 to 2020 (in billions)', Statista, 2019.

[20] 'Risk management guidance: Guidance to help organisations make decisions about cyber security risk', National Cyber Security Centre', 8 August 2018.


ALWARE

To learn more,
contact your AXA XL Cyber underwriter.

S-RM is a global consultancy that delivers breach response, ethical hacking, and cyber risk and governance services.

6316_03/2020