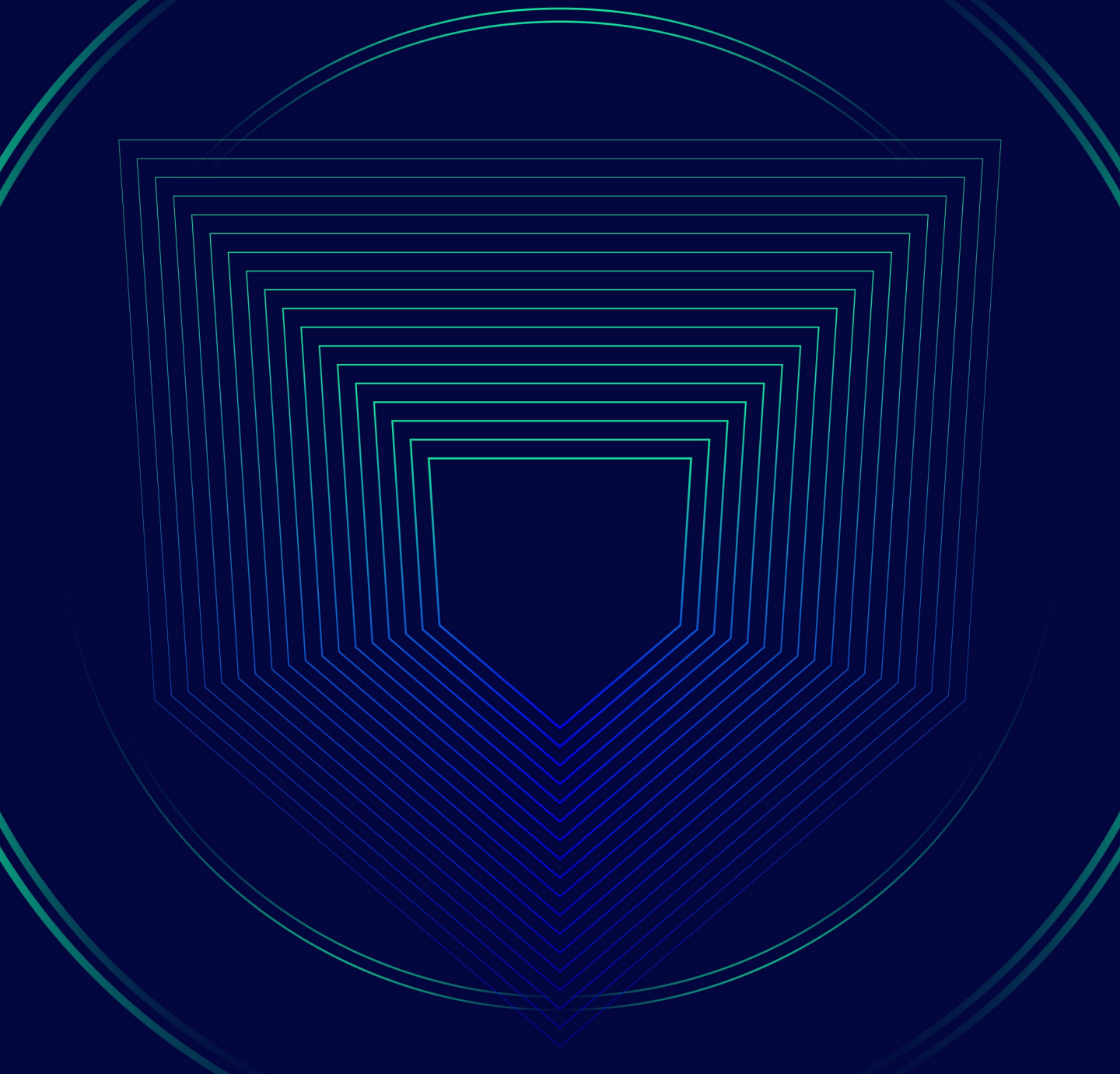
Executive Brief

Cybersecurity in the Financial Industry



Introduction

The societal and economic changes of the 21st century has prompted an increased need for digital solutions to support a world economy and its workforce in adjusting to a new normal. This can be seen in human beings' adaptation to digital technologies to complete everyday tasks. The rapid transition to a highly digitalized world, where businesses, retail, and finance all converge online, has no plan to slow down.

In 2021, it is forecast that technologies within the financial industry will grow as part of our everyday lives and ways of working to improve accuracy and personalization. However, the implications of such a move, although convenient, comes with significant challenges. Especially the threat of cyber-attacks to businesses worldwide. In PwC's 2020 CEO survey, cyber threats were the second most significant concern to CEOs regarding possible threats to their growth potential.

With our lives becoming increasingly digitized and fintech being at the center of how we work, build businesses, attract new customers, and maintain customer and investor relationships, it increases the risk of cyber-attacks, cyber-crime, and losing vital information. And so, this paper will aim to address cyber threats and how we can help strengthen your businesses' knowledge and processes to counteract this 21st century threat.

We will explore:

- The meaning of cybersecurity, what it does, and why it is relevant.
- The latest trends and technology driving businesses into an online sphere and thus the cybersecurity implications.
- Additionally, the paper will provide a helpful guide on the most useful ways for companies to think about cybersecurity, understand the challenges, and ultimately provide clear guidance on how to activate the tools necessary to protect a business in a digital world.

Contents

What is Cybersecurity and why do we need it?

Cybersecurity became well known in the late 1980s, meaning the "measures taken to protect a computer or computer system (as on the Internet) *against unauthorized access or attack*." Yet, cybersecurity is much more than that.

Essentially, cybersecurity is all about protecting the information that is critical to users and businesses. And for many business leaders, the concept of cybersecurity remains an intangible phenomenon. Therefore, this chapter will explore the importance of cybersecurity, what it is, and how it can help alert and prevent different types of threats that your organization may face.

Why is Cybersecurity important?

For personal or monetary gain, malicious online attacks seek to acquire or destroy information and affect businesses' operations with damage to vital infrastructure.

The job of cybersecurity is to stop these attacks from happening. Cybersecurity aims not only to protect computer systems and networks from digital attacks but also to monitor IT assets continuously.

Our thesis is that it is not a question of *whether* a business will be attacked but rather *when* it will be attacked. As businesses evolve, cybersecurity becomes a continuous process of understanding and monitoring the system you are running in tandem with technological development.

To put out fires or secure business continuity?

In many companies, it is common to underfund the cybersecurity teams and their development. Understandably, the work of cybersecurity teams seems too complex for business leaders – or is simply misunderstood. Often, the truth also lies in the struggle of communicating the value of having a well-funded security program – or the risk of not having it. Such struggles can lead to serious gaps between the resources allocated to security and the actual support and strategy needed to protect the business.

As agents for some of the best cybersecurity consultants in the industry, we often experience that business leaders treat security as a liability cost — oftentimes, it is not until the business experiences a security breach that increased support is provided. Thus, creating unforeseen expenses which damage the profit and the company's equity. However, for companies, and especially those in the financial industry, such reactive investment in security support often comes too late – with high costs and harmful media coverage following swiftly.

Suppose you ask the best cybersecurity consultants what cybersecurity essentially is. In that case, they will most likely say it is the work of protecting a company's assets and securing business continuity. And if you are still unconvinced of cybersecurity's value, consider this; statistics show that a hacker attack is happening every 39 seconds*, and furthermore, that 300,000 new malware are created every day.** Worldwide, cybercriminals earn $600 billion every year, which in comparison, is 33% more than what is made on the international drug market. If you want to keep your business from being yet another statistic, read on.

* Source: Security Magazine
** Source: McAfee

4 mega trends that will shape the Financial Industry

As the world becomes more digitally orientated, how we shop, conduct business, or communicate with others all happen online. Thus, we must be wise about what we can do to protect ourselves.

To avoid and counter the broad range of online threats we face, we must look at the latest trends in the fintech industry.

You, your information, and your work are now part of an ever-growing digital world. And consequently, face being exposed to an increasing range of threats. And so, with all these technological changes to the way we conduct business and live our lives, it is more important than ever to make sure we are adequately protected online. So, this chapter will explore how we can use these new technologies safely.

We will explore the latest trends within the fintech industry that we believe will become an increasingly significant part of our daily lives in 2021.

1. Digital Banking – money moving in new circles

The impact of COVID-19 and the acclimatization of society to new software and apps for paying bills and wages has brought forth the rise of online banking. As the need for conventional or brick-and-mortar banks diminishes, more and more people, especially the young, favor the convenience and swiftness of digital banking.

In a recent survey, 44% of 18-34-year-olds across 15 countries enrolled in online or mobile banking for the first time during COVID-19. The move away from paper-based currency will only increase as future generations will be more inclined to accept digital solutions to solve everyday problems. However, online banking does not come without potential threats.

With a range of vital personal information available to potential cybercriminals, digital banks must adhere to strict cybersecurity protocols, artificial intelligence, or biometrics to safeguard you and your details.

2. E-commerce – more shops have gone online

Because of COVID-19, businesses have been forced to bring face-to-face interaction with customers to a halt. Many companies have focused on selling products and goods online to maintain business, protect revenue streams and workers' jobs.

This digitalization has helped keep many companies afloat, and for consumers, it has provided them with an effortless way of shopping. This move has seen an explosion of online sales across many sectors.

An UNCTAD and NetComm survey of 3,700 consumers across several countries saw that online purchases increased by 6-10% across most product categories. This drives change to the way we shop online such as new payment systems to make it more accessible. However, this increased desire for e-commerce solutions to do shopping needs to be adequately protected. The websites you access to complete transactions, your information, including passwords, and the internet usage data you share on these sites, need to be safeguarded with solid cybersecurity measures.

3. New ways to pay for a new world

3A Digital currencies

The Internet is constantly ablaze with the latest trend of cryptocurrencies. Through Blockchain technology, the use of digital currencies allows for transactions to be anonymous and encrypted. To support such protection, they require high cybersecurity levels to protect information, privacy and prevent theft.

3B Contactless payments

We are undergoing a significant shift toward contactless payments. A decreasing desire to carry paper money has lead people toward a form of payment that can be as simple as a tap on a cell phone. Which has seen contactless payments go from an option to a near necessity for digitally aware individuals. Consequently, it has resulted in a growing selection of digital payment platforms from giants like Google, Apple, and WeChat to cater to this rising demand for swift and socially distanced payments. With this, however, contactless payments require stringent cybersecurity measures.

With a growing comfort among customers to purchase goods via their cell phones, safeguarding strategies that protect the individual and their financial details are necessary in case of loss of their phone, or the cell phone being compromised by a cyber-attack. Possible measures to ensure security could be granting access based on facial recognition or fingerprints to provide reliable solutions.

4. Hello AI

Artificial Intelligence (AI) is becoming a more significant part of many industries and ways of life, and fintech is no exception.

How it is used by banks and financial institutions varies. Whether it is providing 24/7 dedicated customer support, fraud prevention systems, or verifying the authenticity of KYC (Know Your Customer) documents, AI provides sophisticated and accurate functionalities. As AI continues to expand and learn, its capacity to support human beings will grow significantly, benefiting consumers. It will soon perform complex automation processes in a secure manner that protects the user. Expect AI to fulfill many vital roles as we progress through the decade.

How to think Cybersecurity

So, with the above-mentioned trends changing the way we conduct ourselves in our daily life, it is the businesses' responsibility to protect their customers from danger. It is of paramount importance for any business to have a secure environment for their customers, their employees, and the company in general. Just like you would want an office or building that is safe, your online security should be a number one priority.

Prioritizing a safe online environment is especially relevant today. COVID-19 speeding up the digitalization process and shifting the workforce to home has created new security complexities that require flexible, innovative solutions to secure this new digital reality. However, innovation comes with the risk of new and unforeseen breaches.

The cybersecurity of businesses fulfills the fundamental role of securing the assets of your company. Thus, good security specialists prevent breaches, the best ensure seamless business continuity when incidents happen. The fact is that breaches are inevitable. By treating security as an integral part of your business life cycle strategy, you can identify, protect, detect, respond – and most importantly – be able to recover at speed and scale..

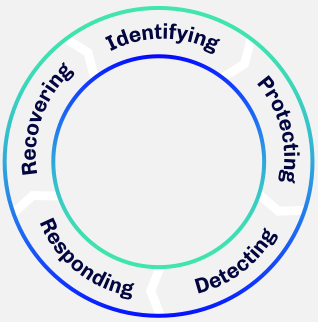
The fact is that breaches are inevitable. You have to make it a priority in your organization before it is too late.

This chapter will explore how organizations can enable a strategic partnership between the security team and the business to unlock improved performance, lower costs, and faster development cycles.

The 5 functions of Cybersecurity

Regardless of the size and complexity of your company's IT organization, there are five functions that should be included in a cybersecurity strategy – and later, plan.

Unfortunately, it is unlikely that your business will never experience breaches, but the damage can and should be minimized by following the practices of:



Identifying cybersecurity risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

Protecting by outlining the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.

Detecting the appropriate activities to recognize the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events.

Responding by including appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.

Recovering with appropriate activities to maintain plans for resilience and restore any capabilities or services that have been impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact of a cybersecurity incident.

Source: NIST

Cybersecurity – an iterative process

A fundamental aspect of securing a business in a digital world is to realize the complexity of such an undertaking. As a multi-layered and ever-growing phenomenon, the challenges posed require constant reassessing and flexible control systems to manage cyber risk. Creating a secure environment at the speed of digital business requires three main elements.

CIA – the elements of Cybersecurity

As suggested by NIST, cybersecurity requires anchoring around three foundational principles represented by the CIA-triad: confidentiality, integrity, and availability.

In this context, confidentiality is a set of rules that limits access to information, integrity is the assurance that the data is trustworthy and accurate, and availability guarantees reliable access to the data by authorized people.

The following is a breakdown of the three key concepts that form the **CIA triad**:

Confidentiality means the measures taken to prevent sensitive information from being taken via unauthorized access attempts. It is common for data to be categorized according to the amount and type of damage done if it fell into the wrong hands. More or less stringent security measures can then be implemented according to those categories.

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire lifecycle. Data must not be changed in transit, and steps taken to ensure data cannot be altered by unauthorized people (for example, in a breach of confidentiality).

Availability means that information should be consistently and readily accessible for authorized parties. This involves appropriately maintaining hardware and technical infrastructure and systems that hold and display the data.

A GUIDING FRAMEWORK
Considering these three principles together can help guide the development of robust security policies for an organization.

When evaluating needs and use cases for potential new products and technologies, the triad helps organizations ask pointed questions about how value is being provided in those three key areas. Thinking of the CIA triad's three concepts together as an interconnected system, rather than as independent concepts, can help organizations understand the relationships between the three.

Source: NIST

Starting the conversation on Cybersecurity

Unfortunately, there remains no single 'magic bullet' solution to securing a digital environment for internet security. Like general societal security, it is dependent on the context of the situation. As well as for digital environments, awareness of the fluctuating waves of trends and new technology help shape the online security process. To meet these challenges, cyber-security strategies with support from a broad range of technological tools and software should be implemented to safeguard your business from ever-changing threats.

Where to begin?

Digitalization starts with understanding your current IT setup to know where and how to deliver digital excellence and improve performance.

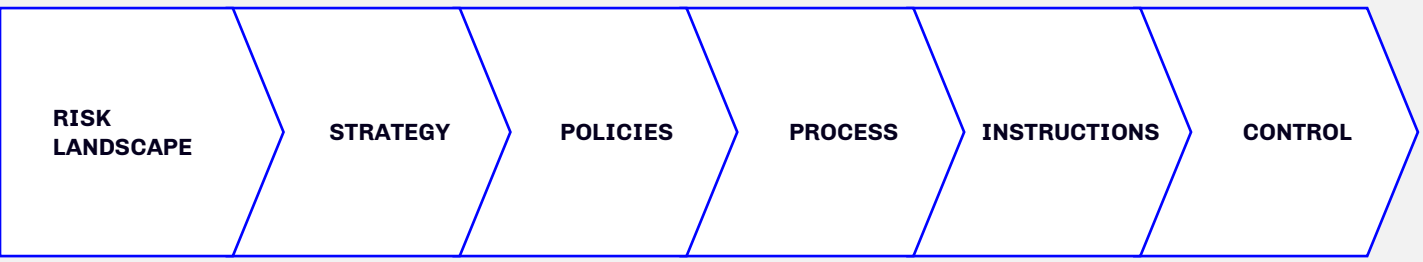
With the ongoing rapid digital and technological development, a strong cybersecurity setup is vital if you want your business to evolve and thrive digitally

.A security plan will help reframe the digital situation to focus more on your business's specific needs. It will attempt to draw attention and address the potential dangers that are likely to affect them and allow appropriate action through its implementation. And to be adaptive to new complexities rather than stuck in a 2-D view of cybersecurity.

When considering a security plan, it must be specific to your company and area of business. It must consider the organizational policies and procedures a business follows and the technical solutions already in place, which allow the company to function and provide security.

To define the plan most suitable for your organization, we have developed a framework to guide you in the process. The framework is based on expert knowledge and insights from 7N Consultants who have been involved in complex security tasks for clients in the financial sector, and 7N Agents who know about the challenges our clients are facing.

7N Cybersecurity Framework



Understanding the risk landscape – leave no stone unturned

It is crucial to map the business environment of your industry and understand what possible risks you can be exposed to.

By investigating and challenging an online security apparatus, providing a wealth of information can bring light to potential points of vulnerability within the system. These can then be dealt with accordingly, and the vulnerabilities can be attributed to the correct level of risk.

If you can predict where online threats may target you, you can build up the response capabilities and prevent putting your organization at risk. This level of preparation will help prevent significant challenges.

Three main areas to focus on when performing a risk assessment in relation to Cybersecurity

REGULATORY RISKS

These focus on a company's requirements to protect the privacy and confidentiality of individuals and their data.

The wealth of information available about an individual's online presence comes under the jurisdiction of external regulatory measures such as GDPR. A security plan must contend with and accept these requirements. The personal data of potentially millions of people needs protection from unauthorized access and abuse from external parties or even organizations. Upholding values like confidentiality, integrity, and stringent authorization regarding access to this information is a business's primary digital security responsibility. This requires businesses to be aware and secure their databases and networks from a potential attack or data breach.

FINANCIAL RISKS

To prevent fraud and embezzlement, organizations need to have controls in place to minimize financial risk. These will support better protection of customers who may be the victims of identity theft or fraudulent behavior as well as the company itself.

Unauthorized transactions completed by stolen identity or credit cards need to be prevented, so steps within a digital security apparatus should support further authentication requirements in the payment process.

OPERATIONAL RISKS

The increasingly digitalized business model may now be conducting most of its operations online. From customer service to logistics, this switch to an online center has helped businesses improve connectivity and convenience, especially during the past year. Furthermore, many people have been relocated to remote working. However, consequently, a security plan must protect an organization at the speed of new digital business solutions and contend with potentially compromising situations brought about by such change. These threats could include intellectual property or confidential information being stolen or disrupted manufacturing operations. A security plan must consider these vulnerabilities and risks and be capable of detecting threats like phishing, denial-of-service attacks, or even industrial espionage and respond swiftly.

For the present and future of businesses, these challenges and the possibility for disruption will only grow as the world becomes more digitally aligned.

Strategy

So, what can a business do to adapt to future changes in its industry? How can it make sure its digital infrastructure is secure?

For businesses, their mission-critical systems now exist in the digital realm and connect to the Internet (even if you think they are not, they likely are). Can they then, as a result, ever be made entirely safe from cyber-attacks? The answer is no. There will always be a threat if there is even the slightest connection to the Internet. As a result, your company requires a cybersecurity strategy. Here are eight steps to follow:

1. Reviews bring progress

For businesses, reviews into their processes help to bring about positive change to their cyber-security. Through analysis, it allows for an improved understanding of your businesses' capabilities to protect itself digitally, which can then be brought about improvement. Furthermore, with emphasis on regularly reviewing your systems, you can avoid your processes becoming outdated.

Technology is rapidly improving at breakneck speed. Doing nothing, letting standards slip, can put you behind your competitors and result in inadequate protection or lack of the tools necessary to deal with modern online threats. A yearly review of your cybersecurity processes should be sufficient. It will allow you to be proactive rather than reactive in safeguarding your business digitally, keeping you one step ahead of digital challenges, and affording you the time and knowledge to best adapt to the future changes that technology will bring to the world of business

2. Identifying weaknesses

By reviewing your processes, you can identify the weak points. By involving those responsible for protecting and maintaining your digital infrastructure, you can make sure they know the most vulnerable parts, as well as reiterate the importance of making sure they are protected. Cause if they were to surrender to a cyberattack and fail, it could potentially jeopardize your business.

Finding weaknesses is not a problem. It becomes one if they are ignored, however.

To prevent the potential targeting of these areas by cybercriminals, you must consider these issues:

- Figure out how to disconnect them from the Internet to the greatest extent possible.
- Reduce their reliance on digital technologies to the absolute minimum.
- And backstopping their monitoring and control with analog devices trusted human beings.

By being proactive, you can face your challenges, understand them, and best prepare your digital infrastructure to cope with threats.

3. Involvement of key stakeholders

A cybersecurity strategy should be a priority for all companies. It allows employees to do their jobs and ensure the company's operations run smoothly and are protected.

The importance of a cybersecurity strategy to adequately protect your company's day-to-day existence should be clearly explained. In particular to those responsible for your company and its decisions - your C-Level and board members. They must understand why cybersecurity is essential, what it allows and what would happen to your company without a functioning means to protect itself. An awareness of the worst-case scenario often drives people to do everything in their power to stop it from happening.

4. Discussion of the company's current direction and future ambitions

Preparation is key. Dialogue between employees and various stakeholders can enable a common understanding of your company's direction within the current day and its future ambitions.

Which, from a cybersecurity perspective, is vital. Knowledge, allowing you to:

- Manage new procedures. Your company may embrace a new digital solution or approach to operating business. You need to be suitably aware of how it works and how best to protect it from viable threats.
- Understand the subtleties of future laws. These you will need to comply with, so your company's cybersecurity processes must both take them into account and follow them accordingly.
- Tech stack. Your company may begin to use new technology within new applications or replace older versions with the latest software—these need to be appropriately understood and vetted so they do not cause a loss of operation.

Preparation and awareness of today's cybersecurity problems, and what the future may hold, helps the management in dealing with these issues.

It affords us the time to find solutions and have them in place, ready for when these challenges surface, which will help protect your company and save you money.

5. Senior management commitment and support

For many Scandinavia companies, cybersecurity is an IT responsibility but rather a strategic priority on C-level and in the Board Room.

With investors' demand for a return-on-investment, governmental regulations, and customer trust on the line, the cybersecurity strategy should be prioritized and supported by the senior management. With the support of senior management, their commitment will make the job far more straightforward. For business leaders, this will require an understanding of the opportunities cybersecurity strategies could provide for their business, how they can reduce risk, and how they can support a broad range of business outcomes. It will reassure senior staff within IT that their decisions to invest in a solid security plan were worthwhile. And ensuring that resources are available for continuous improvements. Remember, hope is not a strategy – thorough analysis, planning, and investment are.

For this, you want to ask your fellow senior management: "What is the worst that can happen to our business in the short and long term?"

6. Consider organizational rules and procedures

For organizations, communication is critical.

Amongst teams and departments, there is a need to be aware of business and strategic objectives to complete core operational tasks and achieve business goals. Clearly defined, concise rules and procedures help the smooth running of organizations. Furthermore, they can guide decision-making, and any choice made can be reasoned and justified, as it is part of an overarching strategy.

And in the case of protecting your business online, rules are pivotal. You know what is required of your security environment, why it is needed, and how to allocate the right resources to manage any potential issues. And ultimately, it will allow for creating technical security solutions that best match your business's needs – and the people that operate and maintain your security system.

7. Using the right technological solutions

When selecting technological solutions, it is important to weigh in many factors.

As technologies develop and ever-shifting trends and threats rise and fall, IT solutions, and those who administer and operate them, must constantly be adapting to deal with change. The primary purpose of technological solutions may be to protect, but it is also imperative that they align with the organization's objectives to drive efficiency and competitiveness. So, it can better support business outcomes across the spectrum of its activities.

But imperatively, cybersecurity technologies are never better than those who implement, maintain, and control the technologies.

One common mistake is to rely too much on the technological solution without knowing how to operate, control, and fix it when breaches strike. This calls for the right people who know how to operate within certain tech environments and within the risk landscape. Cybersecurity technologies are cyber hygiene and only part of the bigger picture.

8. Adoption of laws and industry standards

Gaining an understanding of the laws and regulations that govern any industry is highly recommended – especially those concerning information security. As the digital ecosystem builds, so do the checks and balances to ensure a business has conducted itself correctly. For businesses that maintain a worldwide presence, laws regarding information security can differ from country to country. For example, organizations in EU nations must work following GDPR.

With an ever-increasing amount of data that businesses and websites collect and possess regarding customers, it is vital for these individuals' privacy and security that companies comply with the legal requirements. If they do not, there can be severe consequences. These could be reputational, as lousy business practices can spark a loss of faith and trust from customers or employees, present and future. Or a financial impact upon an organization, as fines are pursued for malpractice and potentially damaging legal costs. If unsure, it is advised to find an expert to help you secure the correct level of compliance regarding information security.

Policies

If your business does not have a cybersecurity policy, employees may not be informed about how to conduct themselves in accordance with the business's security strategy. This could cause potential damage. Find out how to create a cybersecurity policy and plan how you would respond if an incident occurred.

A Cybersecurity policy outlines

- Technology and information assets that you need to protect
- Threats to those assets
- Rules and controls for protecting them and your business

It is essential to create a cybersecurity policy for your business – particularly if you have employees. It helps your employees to understand their role in protecting the technology and information assets of your business. When you prepare your policy, ensure it guides your employees on:

- the type of business information that can be shared and where they can share it
- acceptable use of devices and online materials
- handling and storage of sensitive material.

Develop security policies

A security policy will help organize thinking toward potential risks and choose the right ways to deal with them.

The set and use of policies are ever-changing. For every procedure, a company needs control – and for every technological advancement, security attack, or breach, your policies need to be revised. With a prioritization hierarchy, it is far easier to manage resources and capabilities within the areas requiring the most critical support. For example, internal communication between employees and intellectual property. No one wants to be the victim of online attacks but making employees aware of the new procedures in place will inform and prevent costly mistakes.

But in a digital system of ever-changing challenges, one must manage the risk, accept risk targets, and utilize the resources available to focus the appropriate level of technical security where needed. Awareness and education are crucial - from senior management to staff.

It could be essential to explain why security is changing, its purpose, and how it may affect or change how daily work is completed - which in most cases will not happen. A move toward an open and engaging approach to explaining the new security strategy will hopefully improve understanding and prevent any need to penalize or enforce cybersecurity measures more strictly.

Processes, instructions and control

Once you have done the work of understanding cybersecurity, assessed the risk landscape, and developed a strategy, it is time to plan for what processes to initiate to implement this strategy and how to continue moving forward.

Develop an implementation plan

An implementation plan will help identify what actions are needed to implement the defined security strategy and secure the digital infrastructure of your business.

An organized implementation plan can develop an awareness of the areas that need protection and ensure they are appropriately supported. This step is mainly with people in focus. Who is involved? What is their responsibility for identifying, protecting, detecting, responding, and recovering – on all levels in the organization?

Appropriate security hardware and software tools

There are different technological means, which can be applied to increase a business's security landscape. And the proper specialized hardware and tools will help to protect businesses' online architecture. However, no matter how complex or expensive the tools you invest in are, you need to have a security team of experienced and skilled security people. Because ensuring a company's digital infrastructure and assets is a steady job, which people to monitor all the software implemented in the security environment.

It is like cars; no matter how fancy a car you buy, you still need to drive the vehicle or find someone who can drive it for you. Otherwise, the purpose of having a car as transportation means is not fulfilled, and you cannot use it to get anywhere, as it cannot drive solely on its own – yet at least.

Create a security-minded organization

An organization fully aware of the wide range of potential online threats will make the introduction of a security strategy far smoother.

Through education and training, employees will be better aware in several ways.

1) They will understand how and why they should conduct themselves properly online at work and home.
2) They should be aware of cyber-criminals trying to phish information from them.
3) Being aware of the signs that they may be victims of a cyber-attack prevents further damage or contamination of additional hardware. This knowledge of an organization's security measures should also extend to management.

When a management is aware of security threats, they are also informed of the challenges that are being dealt with, and further, they will know how the methods used to minimize risks help the business run. Furthermore, activities conducted toward a more security-minded organization should include ensuring that the right resources and tools are available to provide security and counter issues.

Perform a security audit

Having a flexible security set-up that supports your business and prepares you to face whatever kind of cyber attack your organization will encounter, entails continuous monitoring of your IT infrastructure and cybersecurity set-up – you must perform controls and be able to adjust.

In the field of security, it is essential to perform control of every policy, process, and tool that is implemented in your security strategy. The security audit or control will tell if the necessary corrective measures and actions are being taken, or if a more significant effort to put right what is wrong is needed.

A security audit involves conducting thorough reviews of a site's infrastructure or a business's shared workspace. This insight can highlight what is successful in enforcing business information security and what needs improvement. Insights develop an understanding which can then lead to improvement.

If you want to know more

We are always more than happy to meet for a virtual cup of coffee. Thus, do not hesitate to get in touch, if you have any questions or want to know more about how 7N can help you along your digital journey.

Helle Førgaard
VP International Business
hefo@7N.com

Theis Eichel
VP Digital Advisory
thei@7N.com

Jakub Strzemzalski
7N Inhouse Remote Development
jast@7N.com

Sebastian Podlesny
7N CEO
sepo@7N.com

Jesper Kolding
VP Denmark
kolding@7N.com

Grzegorz Pyzel
VP Poland
grpy@7N.com

Sources

1. Security Magazine
2. McAfee
3. United Nations Conference on Trade and Development
4. NIST
5. Carnegie – Endowment for International Peace

7N A/S is a global, elite IT consultancy and agency with 30 years market experience in serving all aspects of critical IT projects both within the public and private sector.

We have dedicated ourselves to finding the right match between our consultants and the companies we serve – we believe that is how the best results are created. At 7N, w e have built a professional community of extraordinary people. A community dedicated to achieving professional and personal development. A place where the best gets to play with the best.