Information Security Best Practices: First Steps for Startups and SMEs

Urpo Kaila and Linus Nyman

> *"Many hands make light work."*
>
> John Heywood (1497–1580)
> Writer, musician, and composer

This article identifies important first steps toward understanding and implementing information security. From the broad selection of existing best practices, we introduce a lightweight yet comprehensive security framework with four useful first steps: identifying assets and risks; protecting accounts, systems, clouds, and data; implementing a continuity plan; and monitoring and reviewing. This article is intended primarily for startups and less mature companies, but it is likely to be of interest to any reader seeking an introduction to basic information security concepts and principles as well as their implementation.

Introduction

Consider the scale of malware threats facing a business today. Hundreds of thousands of new malicious files are detected every single day, and almost a third of user computers encountered an online malware attack in 2017 (Kaspersky Lab, 2017). Tens of thousands of phishing sites are created each day (Webroot, 2017). Ransomware, a form of malware that encrypts files on a computer demanding a ransom in exchange for (the possibility of) getting the decryption key, has, according to the European Union's law enforcement organization Europol, "eclipsed most other global cybercrime threats" (Europol, 2017a, see also 2017b). In June of 2017, shipping giant Moller-Maersk was hit by ransomware. Maersk's losses, according to a statement by CEO Soren Skou, were estimated to reach up to $300 million USD (Novet, 2017). The attack wreaked such devastation on the company's IT infrastructure that Maersk employees, with both company email and address systems down, had to rely on using WhatsApp on their personal phones to do their work (Thomson, 2017). Two things are worth noting about the specific form of ransomware Maersk was infected with. First, it was designed to be self-replicating, meaning that every infected computer immediately started looking for new machines to infect. Second, researchers believe the ransomware in question, called NotPetya, was designed not for financial gain, but rather "to spread fast and cause damage" (Mathews, 2017), with little hope for companies of getting their data back even if they paid the ransom (Burton, 2017).

However, malware is just one of many IT-related risks companies face. The abundance of Internet-connected computers in the array of devices known as the Internet of Things has introduced a host of new risks and vulnerabilities (Hypponen & Nyman, 2017). Consider the peculiar case of a North American casino where attackers used an Internet-connected thermometer in a fish tank in the casino lobby to gain access to the casino's network and steal a database containing the casino's high-roller list (Williams-Grut, 2018). Data breaches can carry a high cost both financially as well as to a company's reputation, as Yahoo! experienced first-hand after news broke, in the middle of a corporate merger, that all 3 billion existing Yahoo! accounts had been compromised (Oath, 2017).

As the first author has shown in a previous paper (Kaila et al., 2011), by embedding security in normal operations in a systematic but practical way, a company can easily mitigate many daily cybersecurity risks. However, with all the work involved in starting or running a business, it may seem overwhelming to also find the time to stay informed about the constant stream of news stories about new vulnerabilities, data breaches, and companies getting "hacked" or falling victim to phishing or other online scams. In the face of so many threats, it can be hard to know where to start.

Security professionals have, over the decades, established a number of best practice frameworks and standards, such as the NIST Cybersecurity Framework (NIST,

Information Security Best Practices: First Steps for Startups and SMEs

Urpo Kaila and Linus Nyman

2018a), the OWASP Security Knowledge Framework (OWASP, 2015), and the ISO/IEC 27001 standard (ISO, 2013), to help secure companies and their systems. Although such standards present comprehensive security frameworks, they can be prohibitively cumbersome to a startup or an SME looking to take their first steps towards implementing information security practices. For example, we once met a small software company developing innovative services for university students. This company wished to obtain from the universities limited access to student data to authenticate the students. However, a requirement to grant access was compliance with national information security requirements. Unfortunately, the software company found that the security framework was just so abstract and massive that they withdrew their request. Furthermore, adoption of adequate tools and best practices for security seems often to be constrained by vast and overly complex advice (Renaud, 2016), user interfaces, or requirements and frameworks. An iconic and striking description of the dilemma was presented in an article showing the poor user interface design of a specific version of the PGP encryption client software (Whitten & Tygar, 1996). Security developers had been so focused on theoretical aspects of cryptography that they had failed to communicate the basic concepts of the tool to the users.

This article's first author is Head of Security for the Finnish IT Center for Science (CSC; csc.fi/en) and has spent decades in the field of security, with much of that time focused on developing, implementing, and reviewing security best practices. Our aim with this article is to show how it is possible to implement a lightweight yet fully functional adaption of complex security frameworks mainly intended for large and mature organizations with existing management and compliance governance systems. This article is not intended to be an exhaustive list of all useful best practices; instead, we present an introductory overview of the topic, focusing on a few practices to serve as a starting point for companies who want to take their first steps towards implementing security best practices. Our view and our contribution with this article is based on decades of practice in the field of information security, where we have generally seen success from compact and focused approaches to setting up information security and failure from overly sweeping or too product-oriented approaches to developing security. Our presentation is based on the classical quality circle of "plan – do – check – act" (PDCA; wikipedia.org/wiki/PDCA), which is also the foundation for the more formal frameworks based on security governance.

We want to show how a startup or SME can adapt the best security practices in a comprehensive but lightweight manner. To know from where to start, how to continue, and when to check, managers need to have a frame of reference – a security framework – to see the big picture. In the United States, the National Institute of Standards and Technology (NIST; nist.gov) publishes the Special Publication (SP) 800 series (NIST, 2018b), which presents well-known guidelines and recommendations for the computer security community. The NIST guidelines are of high quality but quite ample. The NIST security framework identifies five stages for security operations: identify, protect, detect, respond, and recover. Here, we present best practices in a similar way, as a series of first steps, but in a more lightweight format aimed at those who are just becoming familiar with the topic. We also see that some advice presented in previous papers (e.g., Rees, 2010) could benefit from being updated to reflect the current IT environments of SMEs and startups, which are heavily based on cloud services and outsourced services.

At its most fundamental level, information security is about awareness. It is about knowing what to protect and how to protect it. And it is about knowing what to do and when, because, despite our best efforts, things will go wrong. The remainder of the article addresses these very topics as a series of practical steps companies can take. First, we discuss identifying assets and risks. Then, we address some critical assets to protect: accounts, systems, clouds, and data. This section also includes examples and suggestions for protecting those assets. We then cover the importance of having a continuity plan, which is essentially a guide to help organizations prepare and respond to various worst-case scenarios. Finally, we discuss the significance of monitoring and review and conclude with a list of recommended reading.

This article is primarily intended for readers with either no experience or very limited experience in information security. Our goal is for the article to be particularly useful for owners or managers of small companies who have not yet implemented security-related practices. The article serves as a general introduction to the topic and may therefore also be of interest to readers seeking a general understanding of security best practices and their implementation.

Information Security Best Practices: First Steps for Startups and SMEs

Urpo Kaila and Linus Nyman

Step 1. Identify Your Assets and Risks

Managers often think of information security as a question of purchasing security-related products or services. While those are important considerations, they should come later. What you need in order to get started with implementing information security is not a credit card but rather a pen and paper. The first step in implementing information security is, quite simply, identifying what to secure. While this may sound trivial, it is perhaps the most difficult, and most overlooked, of all the steps. In our experience, when we have asked managers what their companies most important assets are, few have had ready answers.

In the past, identifying a company's assets and risks was often a more straightforward exercise. Where previously companies might have commonly processed a resource into a refined version of that resource – say, wood to lumber – many companies today process information rather than some physical resource. Listing not just the physical resources and risks to them, but also the "invisible", tacit knowledge, assets, and risks is less straightforward but no less important. Your assets may include a service you provide to your customers or the systems and people who make it possible for you to provide it.

A very clear and understandable, albeit simplified presentation of the relationship between threats, risks, controls, and assets can be found in the OWASP CISO AppSec Guide: Criteria for Managing Application Security Risks (OWASP, 2013). Figure 1 shows how threat agents can use attack vectors to exploit security weaknesses that can and should be mitigated with security controls to avoid, or at least reduce, technical and business impact. A hacker, using freely available exploit tools to gain access to a system with outdated software could cause negative technical and business impacts if access is not properly restricted by a firewall, for example.

There are three key concepts that form a useful foundation for your thinking about and work with implementing information security: confidentiality, integrity, and availability (sometimes referred to as "the CIA triad"). Confidentiality refers to protecting data from being accessed by unauthorized viewers. Integrity refers to maintaining the accuracy and consistency of data over its lifetime. Availability, as the name implies, refers to data being available when needed. At times, there are some challenging balancing acts involved in these key concepts, like the one between confidentiality and availability: how best to ensure everyone who needs access has access, without granting access to those who should not have it.

The output of this first step should be a list detailing assets to be protected and the primary risks to these assets. The goal is not to list every conceivable risk. Rather, it is to list the primary risks you see regarding the key resources you have identified as requiring protection. For example, one way to approach this step is by asking yourself: What IT-related events or mishaps, related to each individual asset, would make our customers and other stakeholders lose trust in our company?

Putting together this list will be beneficial for several reasons. One reason is that it will help you clarify your own knowledge and thinking regarding your company's information security. For any company with customers based in the European Union (EU), another significant

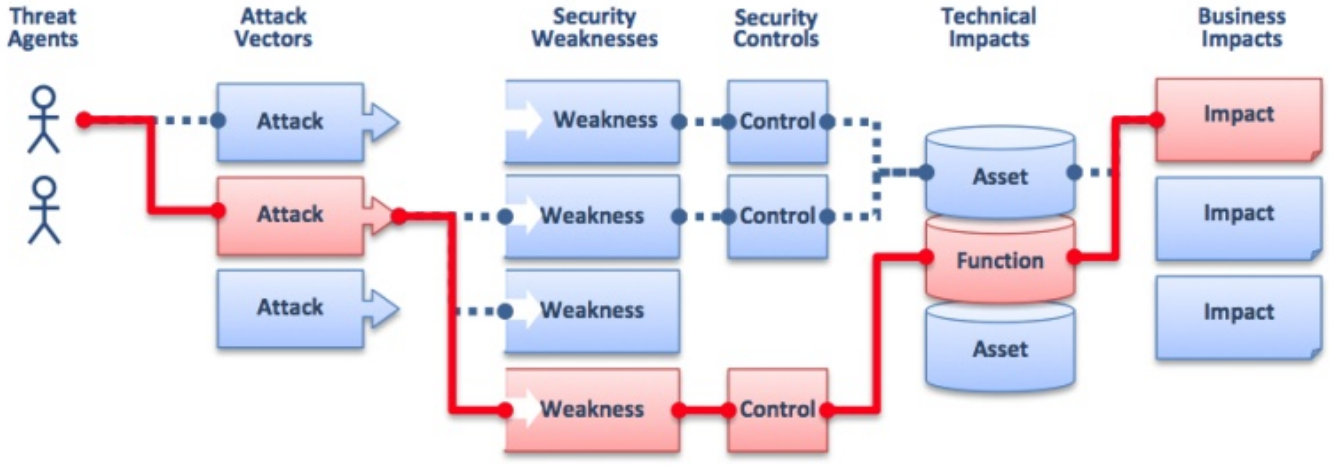

Figure 1. Information security risks, security controls, and impacts (Reprinted from OWASP, 2013: CC-BY-SA)

Information Security Best Practices: First Steps for Startups and SMEs

Urpo Kaila and Linus Nyman

benefit is compliance with the General Data Protection Regulation (GDPR; eugdpr.org). The GDPR requires that companies who process personal data of persons from the EU perform impact assessments of the risk to the rights of the data subjects.

In addition to listing your risks in writing, we recommend that you also agree who in your company is in charge of each of the risks you have identified. When defining risk ownership, be mindful of previous workload and competence. If you have a limited amount of staff with existing skills in information security, offer other employees the opportunity to learn rather than by default making one IT-knowledgeable person the owner of all identified risks.

Some examples of common IT-related risks include:

- An account is compromised (e.g., a staff member's password is guessed or their credentials are phished – more about this later).
- A service is not available. Whether it is a service that your company uses or a service that your company provides to your customers, a service not being available (when it should be) is an IT risk you should be aware of and plan for.
- Data is lost. Data loss could be accidental, a result of poor maintenance, or through malicious intent.
- A system is infected by viruses or other malware. These are the things many people closely associate with information security. They are most definitely an important consideration, but they are not the only consideration in putting together this list.

Table 1 shows a simple example of how you can list and manage your risks. Additional examples and guidelines can be found in the Recommended Reading section at the end of this article. In particular, we highlight the Risk Assessment Template by the WISE Community (wise-community.org/risk-assessment/).

2. Protect Your Accounts, Critical Systems, Clouds, and Data

The spectrum of risks to IT-related systems is broad. So, we will focus on a few topics of broad relevance as a starting point for implementing information security: accounts, critical systems, clouds, and data. A more comprehensive list of assets to protect, relevant to your specific company, should be derived from the list you drafted in Step 1.

Table 1. Example of a lightweight security framework for a startup or SME

Asset	Risks			Risk Owner	Mitigation / Control	Reviewed (Date/Initials)	Review Schedule
	Leak of Confidential Information	Loss of Data	Service Down				
E-commerce portal	Medium	High	High	Marketing Manager	Service Level Agreement with fines, monitoring	Sep 18 N.N.	Annual
R&D content	High	High	Medium	CTO	Internal, mirrored server, strong authentication	Aug 18 M.M.	Quarterly
Customer database	High	High	Medium	Sales Manager	Service Level Agreement with fines	Nov 1 O.O.	Weekly
HR database	High	Low	Low	HR Manager	Internal, mirrored server		Daily
Internal documents	High	Medium	Medium	CTO	Internal, mirrored server, strong authentication		
Contract database	Medium	Medium	Medium	Sales Manager	Backup with verified restore		
Financial services	Low	Low	Medium	CFO	Service Level Agreement		
CRM service	Medium	Medium	Medium	Sales Manager	Service Level Agreement with fines		
Identify management system	High	Medium	High	CIO	Internal, mirrored server, strong authentication		

Information Security Best Practices: First Steps for Startups and SMEs

Urpo Kaila and Linus Nyman

Your goal here is to mitigate risk. Although the CIA triad of confidentiality, integrity, and availability, discussed in the previous section, offers a helpful way to think about and address information security issues, there are additional important tools to use in mitigating risk. These are called "controls". Controls can be divided up into three categories: preventative, detective, and responsive. Preventative controls seek to prevent unwanted things from happening. Detective controls help detect when unwanted things are happening. Responsive controls are controls that take effect after an unwanted incident has taken place; their goal is to help mitigate damage and get things back to normal.

Controls help mitigate risk but can themselves involve a balancing act. A concrete example, when deciding what controls to implement, is the balance between security and usability. Unfortunately, making something more secure often leads to it being less user-friendly, or at least somewhat more time-consuming to access or use. For example, implementing multi-factor authentication (something we will discuss shortly) makes an online account considerably more secure, but makes it take a while longer for the user to log in to their account.

Protect your accounts

Having an attacker gain control of an account can open up an organization to serious risk, particularly if the account in question has administrative rights. Think of it like losing your keys: the more keys on your keychain, the more access a thief will have if they get hold of them. An attacker can try to gain hold of an account by simply guessing a user's password. Or, they can try to gain access to an account by tricking the user into giving up this information – this is called "phishing". Important considerations in securing accounts are requiring strong passwords, educating employees about phishing and similar attacks, and – where possible – implementing multi-factor authentication:

1. *Require strong passwords:* Conventional wisdom regarding passwords has taught us that we can improve password strength by including a mixture of special characters, numbers, and a mixture of uppercase and lowercase letters. While such increased complexity is beneficial, password length is a more important consideration. In fact, pass*word* is in itself an unfortunate choice of word. It would be better to speak of pass*phrases,* or "secret sentences" – the idea being that the most important goal of a password is to be long. Complexity is good, but its significance comes second to that of length. At a minimum, we recommend 12-character passwords. A good rule of thumb for a password is that it should be hard to guess but easy to remember. For example, "DogsDanceDiscoDaily" is both easier to remember and a stronger password than "p@s5w#rd12". A second consideration regarding passwords is the importance of their being unique to an account. Reusing passwords is a common and very dangerous practice. The reason it is a huge risk is that data breaches have become common. If a password you reuse in multiple accounts is leaked online in a data breach, criminals can try this password on other accounts and potentially access an important work account even though the data breach was entirely unrelated to it. Default passwords (i.e., passwords or password patterns preset by a device manufacturer) are equally a risk and should be changed when possible. Such passwords can often either be easy to guess or can be found online. Both commonly used passwords as well as default passwords can be expected to be included in toolkit dictionaries, which are huge lists of commonly used passwords that criminals can use to attempt to break into accounts.

2. *Learn to recognize phishing and other common cons:* Another common attack is to try to trick a user into giving up login information or other sensitive data through phishing. Sites are made to look identical to trusted sites, with the goal of tricking users into handing over to the criminals their login information, credit card number, or other sensitive data. Another example of a popular scam is the CEO scam, in which criminals trick a company employee to pay a bogus invoice by attaching it to an email made to look like it is from the CEO. Artificial intelligence can detect many forms of phishing and scams, but not all. Email sender information is easy to spoof, meaning it is trivial to make an email look as though it was sent by someone else. Links can be made to look like they lead to a real site but actually lead to a phishing site. And only the URL of a website – not what the site looks like – actually tells you where you are. It is very important for all employees to have a basic grasp of such tricks and how to spot them.

3. *Implement multi-factor authentication:* Another good way to secure accounts is to implement multi-factor authentication, sometimes known as two-factor authentication or 2FA. This means that, in addition to a password, you will also need to authenticate yourself through a second means, or factor. This can be, for instance, a USB dongle or through a key (password) sent to your cellphone. Therefore, if a criminal manages to guess or phish a password to an

Information Security Best Practices: First Steps for Startups and SMEs

Urpo Kaila and Linus Nyman

account, you can still be safe as long as they cannot access your second factor.

Box 1 lists examples of actions to take and controls to implement to protect accounts.

Protect your critical systems
Here, it is useful to distinguish between systems, data, and services. For example, you can have a computer or a corresponding virtual machine, files containing data, and a running service for processing customer orders. A laptop in and of itself is not mission critical. However, mission-critical data might exist solely on one laptop, which is not advisable at all security-wise.

Common critical IT systems to most business are the invoicing, sales, logistics, or customer management systems and all the data they contain. Also, be mindful of whether any of your mission-critical IT systems rely on so-called legacy systems, meaning outdated hardware or software. An additional consideration in identifying risks and devising security is being aware of whether any of these systems are such that only one or a few people know how they work. Is there a critical function that ceases to function when any one single person is no longer there to manage it?

Box 2 lists examples of actions to take and controls to implement to protect critical systems.

Protect your cloud
Companies are becoming increasingly reliant on cloud providers for their data storage. Make sure you have written agreements with all your cloud providers. Before committing to a provider, always check the cloud provider's rights and responsibilities. Some important considerations are: What do they do to safeguard your data? What happens if they lose your data? It could be that they will have to pay a fine if they lose your data, but that will be little consolation to you if business-critical information goes missing. Also, check their promised availability. Availability refers to how reliably their service is accessible, and is commonly measured in nines (i.e., "How many 9s?"): 90% availability is considered one nine. This would translate to 36.5 days of downtime per year. So, 99% is two nines, 99.9% is three nines, etc. A guarantee of six nines means, at most, half a minute of downtime per year. Estimate the value/risk to your business of cloud downtime and choose accordingly.

If you are a small or medium-sized company, it probably is not worth your time to even imagine that you could negotiate a unique and favourable deal for yourself with

Box 1. Practical actions to protect accounts

- Have minimum requirements for password length. For example, require all passwords to have at least 12 characters.
- Implement multi-factor authentication, at least on email and other critical accounts.
- Only those who need accounts should have them. Be mindful of test accounts – make them as secure as other accounts (e.g., with strong passwords) and delete them once they have served their purpose.
- Implement mandatory information security training for all employees (e.g., to teach them how to recognize phishing and other scams).
- Remove accounts when no longer needed.
- Restrict rights on accounts to what is needed.

Box 2. Practical actions to protect critical systems

- Ensure that you install security patches in a timely manner.
- Shut down all unnecessary services on your hosts. For example, shut down a local email service if you do not need it.
- Do not make your mission-critical infrastructure directly available on a public network.
- Implement layered defence. For example, do not expose confidential information directly to public networks.
- Ensure that all accounts are unique and can be connected to a person. Do not share accounts.
- Authenticate all users. Everybody must log in with a password or with a key.
- Log access and keep your logs on a separate host.
- Restrict network access with firewall rules, both on the network level and on host or service levels

Information Security Best Practices: First Steps for Startups and SMEs

Urpo Kaila and Linus Nyman

the likes of Microsoft or Amazon. But even then, do make sure any deal you get from them is sufficiently favourable (e.g., ask "How many 9s?") and actually read the agreement and know what you are getting. If you are looking into buying a service from a smaller company, check not only your rights and the supplier's rights and responsibilities but also the supplier's accreditations. The ISO/IEC 27001 certification for information security management systems is the most valued international certification, and all serious cloud providers have been awarded this certification.

Box 3 lists examples of actions to take and controls to implement to protect cloud-based assets.

Protect your data

Here, it is useful to circle back to the original point of Step 1: before we can secure something, we must know what we want to secure. Unfortunately, with young companies, a lack of knowledge about their data – what exactly it is and where it is located – is quite common. For example, personal and corporate email accounts may be used interchangeably, and things like orders, invoices, and commitments may be distributed among them. Companies should try to keep personal and private accounts separated. If you always have to start by searching your email to find what data you are looking for, you – and your company's information security – would benefit from better structuring.

Whether your data is in the cloud or on your own hard drives, one cannot overstate the importance of backups and the ability to recover from anything – from ransomware to a hard drive failure or a fire. A crucial but often overlooked step is testing your backup system to make sure things work in practice, not just in theory. You can further improve your information security by encrypting data before uploading it to the cloud.

Box 4 lists examples of actions to take and controls to implement to protect data.

Box 3. Practical actions to protect cloud-based assets

- Check what your provider promises you on security.
- Marketing materials are not enough – you should require security agreements.
- Make sure your providers have solid privacy policies.
- Check what guarantees are provided on the availability of the service and of your data.

Box 4. Practical actions to protect data

- Write down what critical data you need to be able to restore to recover your business.
- Have an automatic backup system in place.
- Test the backup system regularly, for example weekly, to ensure that the data really is being backed up and can be successfully restored.
- Check the integrity of your files and databases, too. Can you actually read what is restored?
- Mark and classify your data and your property. Write "confidential" or "internal" if the file is not public.
- Write a security policy for your staff. Company systems are intended only for business use; inappropriate use and abuse or causing harm is prohibited.

3. Make a Continuity Plan

Even after taking significant steps to ensure things do not go wrong, it is still important to have in place a disaster recovery plan prepared in advance for when things, despite your best efforts, go wrong anyway. This step ties in with the previous step on protecting your various assets by addressing what to do if those protections fail. Making a continuity plan can be perhaps the most effective way to communicate information security in practice to your staff and other stakeholders, as it can make the abstract controls understandable for people with less or no knowledge of the affected system or the incident that might have affected it.

A continuity plan can be implemented in different ways. The basic concept is to secure your business operations even in the case of various disturbances or unfortunate events. One approach is to have a set of controls in place. This could be lists of fallback options, as the example in Table 2 shows. This example for a business continuity plan shows a concise, simple template for writing your contingency plan, which is based on a

Information Security Best Practices: First Steps for Startups and SMEs

Urpo Kaila and Linus Nyman

version in use at the Finnish IT Center for Science (CSC). The template in Table 2 gives a sense of the recommended level of granularity for a continuity plan. However, an actual plan would be less generic and should include specific services and the names of the individuals responsible for them. So, should something happen to a given critical function, you would have a "plan B" in place to provide that function. Or, if data is lost, you would have a recovery plan ready, describing how to recover that data. Also, for critical services, it is good to have a disaster strategy. If the customer portal is down, it would be good to at least be able to redirect traffic to another site, saying that the service is temporarily down but recovery is under way.

4. Monitor and Review

This is an important yet often overlooked part of a company's information security. Even with the best of plans in place and the most advanced of security products securing your systems, it is still important to continuously monitor and review the situation. This may be challenging for a small company to do continuously, but you should try to have at least some security-related metrics that you keep track of, which can give you some insight into the situation and its trends or evolution over time. Some examples of parameters for security metrics could be service availability ("How many 9s?"), the amount of malware detected, security events and security incidents, and the number of security agreements you have signed.

Monitoring is also useful as far as compliance is concerned: the data you have gathered is something to mention, or show, should you be asked about your company's insights into its own information security. An additional benefit of monitoring is that having logs is crucial in the event of a compromised system. Without logs, you will be left guessing what went wrong and why. Your logs will not only enable uncovering what happened, but it will also inform your decision regarding how to respond to an incident.

There are many other things that would be useful to monitor and examine, but which may require more familiarity with information security – and in particular computers and networks – than people in your company may have. A further important action, particularly if in-house knowledge is limited, is to have an expert from outside of one's company examine your security. They can be hired to instruct you regarding how to secure your systems as well as to test your product, company, or network for vulnerabilities.

Table 2. Example of a concise business continuity plan

Business Continuity Plan for Service X
1. Purpose and scope of the plan
2. Description of Service X
2.1 Description
2.2 Network diagram
2.3 System components
2.4 Dependencies (of other services and to other services)
3. Contact information
3.1 Administrative staff
3.2 Customers and other stakeholders
3.3 Subcontractors and agreements
4. Risk and impact analysis
4.1 Risk analysis
4.2 List of related security controls
5. Incident management guideline
5.1 Roles
5.2 Crisis communication
5.3 Contact with authorities and CSIRT teams
6. Disaster recovery plan

Information Security Best Practices: First Steps for Startups and SMEs

Urpo Kaila and Linus Nyman

Conclusions

Information security is about knowing what to protect and how to protect it. If you understand your company and what value you offer to your clients, then you have already taken an important first step towards implementing information security. Rather than feeling intimidated by the breadth or complexity of the myriad potential weaknesses or vulnerabilities your company or its IT system is facing, focus instead on the concrete tasks involved in outlining a plan for how to protect your business and the data of your customers and your staff. Then implement that plan. If, or rather when, you face a security incident, remember: don't panic. Stick with the security framework you have tailored for your own company and face the threats. During the incident, you can then, as the United States marines slogan says: "improvise, adapt, and overcome".

When you have created a minimum feasible security model for your services and your systems you should advance to continuously improve your security by balancing risks and the costs in money, time, and usability of available security controls. You could, for example, consider deploying controls for proactive intrusion detection and prevention (IDS/IDP), identifying advanced persistent threats (APT), or evasions of your firewall rules. Many of these functions can also be obtained from a service provider.

Adequately managed information security is part of the basic governance of any business, and it is also a good and necessary investment. In addition to mitigating your risks, you also need security to show compliance. Should things go wrong, you have at least made a reasonable effort to protect your business and the data of your customers and your staff. It is also a good idea to have somebody else to review your security. A focused network scan for vulnerabilities, penetration testing of your critical services, or a walkthrough on how you make changes in your services (change management) can help you to identify issues and patch vulnerabilities before a malicious party finds them. Proactive security is also a very good way to show due diligence in security matters. However, no control is bulletproof, especially when considering potential trade-offs with usability and the need to keep costs at a reasonable level.

But you need to begin with the basics first. If you follow the basic steps we have presented in this introductory article, you are already well on your way to ensuring adequate information security for your business. Starting with best practices when you are small and growing them as you grow is an excellent way to implement and maintain information security practices. The steps we have outlined here are important, but they are just the beginning. Once you feel you have understood and implemented them, please dive deeper into the topic. As your company and your understanding of information security principles grow, you may also decide to adopt more comprehensive frameworks, as highlighted in the recommended reading list below.

Recommended Reading

- 10 Steps to Cyber Security (UK National Cyber Security Centre)
  https://www.ncsc.gov.uk/guidance/10-steps-cyber-security
- OWASP Top 10 Most Critical Web Application Security Risks (Open Web Application Security Project)
  https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- NIST Special Publication 800-Series (US National Institute of Standards and Technology)
  https://www.nist.gov/itl/nist-special-publication-800-series-general-information
- Security for Collaborating Infrastructures Trust Framework (WISE Community)
  https://wise-community.org/sci/
- Risk Assessment (WISE Community)
  https://wise-community.org/risk-assessment/
- Cybersecurity Best Practices (Center for Internet Security)
  https://www.cisecurity.org/cybersecurity-best-practices/
- *Carry On: Sound Advice from Schneier on Security* (Bruce Schneier)
  https://www.schneier.com/books/carry_on/

Information Security Best Practices: First Steps for Startups and SMEs

Urpo Kaila and Linus Nyman

About the Authors

Urpo Kaila is the Head of Security for CSC – the Finnish IT Center for Science. His background in the information security industry, with long experience in handling security incidents as well as developing solutions for information security and data protection. He has been responsible to achieve the valued ISO/IEC 27001 information security management certification for CSC and is a steering committee member in security groups for some European Research Infrastructures, such as WISE and GÉANT SIG-ISM. Urpo holds the professional international information security certificates CISSP, GCIH, GCED, CISM, and ISO 27001 Lead Auditor. He also holds a Master's degree from the Hanken School of Economics. His research focuses on best practices in information security and data protection.

Linus Nyman is an Assistant Professor at the Hanken School of Economics in Helsinki, Finland, and an Adjunct Research Professor in the Technology Innovation Management (TIM) program at Carleton University in Ottawa, Canada. He has lectured on a range of topics, including information security and privacy, information systems science, corporate strategy, and open source software development. His current research focuses on information security and privacy, which are topics he also covers in a blog for the Finnish daily newspaper *HBL*. Linus holds a PhD and a Master's degree, both from the Hanken School of Economics.

References

Burton, G. 2017. NotPetya Is, er, Not Ransomware, Victims Unlikely to Get Files Back. *The Inquirer,* June 29, 2017. Accessed October 22, 2018: https://www.theinquirer.net/inquirer/news/3012890/notpetya-ransomware-intended-to-destroy-not-extort-money

Europol. 2017a. *2017, The Year When Cybercrime Hit Close to Home. Press release.* The Hague, Netherlands: European Union Agency for Law Enforcement Cooperation (Europol), September 27, 2017. Accessed October 22, 2018: https://www.europol.europa.eu/newsroom/news/2017-year-when-cybercrime-hit-close-to-home

Europol. 2017b. *Internet Organized Crime Assessment (IOCTA) 2017 Report.* The Hague, Netherlands: European Cybercrime Centre; European Union Agency for Law Enforcement Cooperation (Europol). Accessed October 22, 2018: https://www.europol.europa.eu/iocta/2017/index.html

Hypponen, M., & Nyman, L. 2017. The Internet of (Vulnerable) Things: On Hypponen's Law, Security Engineering, and IoT Legislation. *Technology Innovation Management Review,* 7(4): 5–11. http://doi.org/10.22215/timreview/1066

ISO. 2013. *ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements.* Geneva: International Organization for Standardization (ISO). https://www.iso.org/standard/54534.html

Kaila, U., Passerini, M., & Virtanen, J. 2011. Metrics and Best Practices for Host-based Access Control to Ensure System Integrity and Availability. In *Proceedings of the Cray User Group Conference (CUG 2011),* May 23–26, 2011, Fairbanks, Alaska. https://cug.org/5-publications/proceedings_attendee_lists/CUG11CD/pages/1-program/final_program/10.monday.html

Kaspersky Lab. 2017. Kaspersky Security Bulletin: Overall Statistics for 2017. *Kaspersky Lab,* December 14, 2017. Accessed October 22, 2018: https://securelist.com/ksb-overall-statistics-2017/83453/

Mathews, L. 2017. The NotPetya Ransomware May Actually Be A Devastating Cyberweapon. *Forbes,* June 30. Accessed October 22, 2018: https://www.forbes.com/sites/leemathews/2017/06/30/the-notpetya-ransomware-may-actually-be-a-devastating-cyberweapon/

NIST. 2018a. Cybersecurity Framework. *National Institute of Standards and Technology (NIST),* April, 2018. Accessed November 1, 2018: https://www.nist.gov/cyberframework

NIST. 2018b. NIST Special Publication 800-Series General Information. *National Institute of Standards and Technology (NIST),* May 21, 2018. Accessed November 1, 2018: https://www.nist.gov/itl/nist-special-publication-800-series-general-information

Novet, J. 2017 Shipping Company Maersk Says June Cyberattack Could Cost It Up to $300 million. *CNBC,* August 16, 2017. Accessed October 22, 2018: https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html

Oath. 2017. Yahoo Provides Notice to Additional Users Affected by Previously Disclosed 2013 Data Theft. Press release. *Oath,* October 3, 2017. Accessed October 22, 2018: https://www.oath.com/press/yahoo-provides-notice-to-additional-users-affected-by-previously/

OWASP. 2013. CISO AppSec Guide: Criteria for Managing Application Security Risks. *Open Web Application Security Project (OWASP),* September 18, 2013. Accessed October 22, 2018: https://www.owasp.org/index.php/CISO_AppSec_Guide:_Criteria_for_Managing_Application_Security_Risks

OWASP. 2015. OWASP Security Knowledge Framework. *Open Web Application Security Project (OWASP),* September, March 11, 2015. Accessed October 22, 2018: https://www.owasp.org/index.php/OWASP_Security_Knowledge_Framework

Rees, J. 2010 Information Security for Small and Medium-Sized Business. *Computer Fraud & Security,* 2010(9): 18–19. https://doi.org/10.1016/S1361-3723(10)70123-8

Information Security Best Practices: First Steps for Startups and SMEs

Urpo Kaila and Linus Nyman

Renaud, K. 2016. How Smaller Businesses Struggle with Security Advice. *Computer Fraud & Security,* 2016(8): 10–18. https://doi.org/10.1016/S1361-3723(16)30062-8

Thomson, I. 2017. NotPetya Ransomware Attack Cost Us $300m – Shipping Giant Maersk. *The Register,* August 16, 2017. Accessed October 22, 2018: https://www.theregister.co.uk/2017/08/16/notpetya_ransomware_attack_cost_us_300m_says_shipping_giant_maersk/

Webroot. 2017. Quarterly Threat Trends. *Webroot,* September 2017. Accessed October 22, 2018: https://www.webroot.com/us/en/business/resources/threat-trends/sept-2017

Whitten, A., & Tygar J. D. 1996. Why Johnny Can´t Encrypt: A Usability Evaluation of PGP 5.0. In *Proceedings of the 8th USENIX Security Symposium:* 169–184. August 23–36, 1999. Washington, DC. https://www.usenix.org/legacy/events/sec99/full_papers/whitten/whitten_html/index.html

Williams-Grut, O. 2018. Hackers Once Stole a Casino's High-Roller Database Through a Thermometer in the Lobby Fish Tank. *Business Insider,* April 15, 2018. Accessed October 22, 2018: https://www.businessinsider

Citation: Kaila, U., & Nyman, L. 2018. Information Security Best Practices: First Steps for Startups and SMEs. *Technology Innovation Management Review*, 8(11): 32–42. http://doi.org/10.22215/timreview/1198

Keywords: information security, cybersecurity, best practices, startups, SMEs, risk management

Technology Innovation Management Review

timreview.ca

Academic Affiliations and Funding Acknowledgements

Canada

The Federal Economic Development Agency for Southern Ontario (FedDev Ontario; feddevontario.gc.ca) is part of the Innovation, Science and Economic Development portfolio and one of six regional development agencies, each of which helps to address key economic challenges by providing regionally-tailored programs, services, knowledge and expertise.

- *The TIM Review receives partial funding from FedDev Ontario's Investing in Regional Diversification initiative.*

Carleton UNIVERSITY

TIM

Technology Innovation Management (TIM; timprogram.ca) is an international master's level program at Carleton University in Ottawa, Canada. It leads to a Master of Applied Science (M.A.Sc.) degree, a Master of Engineering (M.Eng.) degree, or a Master of Entrepreneurship (M.Ent.) degree. The objective of this program is to train aspiring entrepreneurs on creating wealth at the early stages of company or opportunity lifecycles.

- *The TIM Review is published in association with and receives partial funding from the TIM program.*