Executives and Entrepreneurs

A practical guide to cyber security for the entrepreneur

Chief Investment Office GWM | **25 July 2019** 4:30 pm BST
Caroline Simmons, CFA, Strategist; **Sundeep Gantori**, CFA, CAIA, Analyst; **Alexander Stiehler**, CFA, Analyst

- Cybersecurity ranks as one of the top three concerns for investors and business owners, and the number of cybersecurity incidents is rising by 20%-30% per year. Globally, the average total cost of a data breach in 2018 stood at USD 3.86 million.
- Small and medium sized enterprises are at least as much as risk as the headline-grabbing larger companies.
- This report provides ten top tips for keeping your business cyber secure, as well as an interview with a cybersecurity expert. We look at some of the most common forms of cyber attack, how to limit costs and the likely future evolution of risks.

Source: UBS

Introduction

In a recent global UBS Investor Survey, cybersecurity ranked as one of the top three concerns for investors and business owners.

According to Interpol, cybercrime refers to crimes against computers and information systems, where the aim is to gain unauthorized access to a device or deny access to a legitimate user.

According to Bloomberg Intelligence, global cyber security incidents are rising by 20%–30% per year. We expect this trend to continue and view small and medium-sized companies at just as much at risk as anyone else. According to Beaming and Opinium, almost two-thirds of UK businesses with between 10 and 49 members of staff were targeted by cyber criminals in 2018. Entrepreneurs need to be on top of cyber risks and security – it's a question of "when" not "if" an attack happens.

In this report we identify and explain some of the most common forms of cyber attack, and how they happen. We explore how to limit the cost of impact, increase detection rates, and look at the potential evolution of cyber risks. We also consider how poor cyber hygiene and security can affect your company's valuation.

We also suggest ten top tips for keeping your business cyber secure, and feature an insightful interview with a cybersecurity expert which offers practical tips for entrepreneurs.

What is cybercrime?
In today's digital world, most of us have become more interconnected than ever before. However, this increased connectivity also exposes us to increased cybercrime. According to Interpol, cybercrime refers to crimes against computers and information systems where the aim is to gain unauthorized access to a device or deny access to a legitimate user. Cybercrime has a long-lasting impact on individuals and corporates. For an individual, cybercrime can expose confidential data, which can have a huge emotional and financial impact. At the corporate level, cybercrime can bring the entire IT infrastructure to a standstill, and expose trade secrets, customer details and other critical data. This can even result in the downfall of a business. Cybercrime has broader consequences than merely exposing the IT vulnerabilities of the affected party. It damages trade, competitiveness and innovation at the macro level. Employment is also threatened, as repeated cyber threats can jeopardize new investment and job creation. Despite the broad-based implications of cyber security risks, we believe many individuals and entrepreneurs are ill-prepared for cybercrime as they still need to beef up their security infrastructure to prevent breaches.

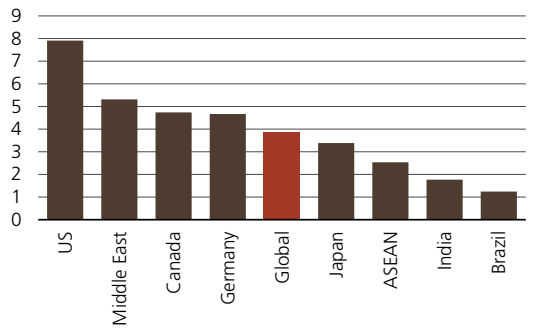
Size of the cybercrime market
According to Bloomberg Intelligence, cyber security incidents are rising by 20%-30% every year, a trend we expect to continue, which creates a significant economic impact. According to a study by IBM Security and Ponemon Institute, the average global cost of a data breach in 2018 was USD 3.86 million. As shown in Fig.1, the average cost is disproportionately higher in the US, Middle East and Canada, while the average cost was lowest in Brazil and India.

Growth of cybercrime past and future
Driven by a 20%-30% rise in cybersecurity incidents, we believe the global cybercrime market is rising in value by a double–digit percentage rate every year. This is also supported by rising average cost of data breaches which, according to IBM Security and Ponemon Institute, has risen from USD 3.62m in 2017 to USD 3.86m in 2018. The increase in the cost of cybercrime is also driven by a change in the motivation of the hackers. We believe cyber-attackers' intentions have also shifted from gaining notoriety to benefiting financially or politically.

Exposure of small and medium sized enterprises to cybercrime
We've all read the headlines about large companies that have been the victims of cybercrime. However, don't assume because you are a small or medium-sized company that you won't be targeted. According to a survey conducted by internet service provider Beaming and market research group Opinium, "almost two-thirds of UK businesses with between 10 and 49 members of staff were targeted by cyber criminals in 2018, and each attack cost the business targeted an average of £65,000."

Common external attacks in smaller companies relate to phishing for personal data or system log in details to commit fraud, as well as ransomware attacks. In particular, payment controls should be closely monitored and secured. It is surprisingly common for companies to make payments to criminals who are mimicking their vendors.

Fig. 1 Average total cost of a data breach by regions
In USD mn



Source: IBM Security, Ponemon Institute LLC, (2018 Cost of a Data Breach Study: Global Overview), UBS

In some instances, smaller companies also need to focus on staff controls and training and the risk of disgruntled employees setting off elsewhere taking company or client data with them.

Different industries will face different risks. For example, service companies which take payments or deal with large numbers of customers are particularly responsible for keeping the personal data safe under the GDPR rules. Manufacturing companies for example, who use lots of smart monitoring on the factory floor will need to focus more on the safety around the Internet of Things. A good starting point is always to be in touch with your industry regulatory or industry body to find out what specific regulations and risks apply to your industry.

Types of cybercrimes and some real life examples
There are many different types of cybercrime. We highlight the most common examples in this report. The following list is not exhaustive, but Fig 2. shows a broader list.

Fig. 2 Entrepreneurs can get caught out by cyberattacks if not unprotected

Source: UBS

a) **Phishing**: Phishing is one of the most common forms of cyberattack. Sensitive information is collected by hackers disguised as a trustworthy entity usually through deceptive emails or websites, but sometimes also by telephone. In 2009, the FBI called Operation Phish Phry the largest phishing case ever, following the large-scale theft of bank and credit card customers' information.

b) **Spyware**: Spyware is a form of malware or malicious software that infiltrates computing devices, stealing sensitive information. CoolWebSearch is one of the best-known spyware programs and first appeared in 2003. The program changes the homepages of the affected computer browsers to CoolWebSearch and creates pop-up ads.

c) **DDoS attack**: A distributed denial of service (DDoS) attack is one of the most common ways to crash the websites of affected parties. Bots disrupt the normal traffic of an online service by overwhelming the target with a flood of internet traffic. In 2018, Github, a popular developer platform, was hit with one of the largest DDoS attacks ever, with an onslaught of online traffic that at one point clocked 1.35 terabits per second. This mode of attack is also common in geo-political cyber conflict.

d) **Advanced Persistent Threats**: Advanced Persistent Threats, or APTs, are some of the most complicated online attacks. The source or the technique of the attack is very difficult to track and may go undetected for many days. The Marriott Starwood breach, where up to 500m customers were affected, is an example of an APT attack.

e) **Password or brute force attack**: While these kinds of attacks are a very old form of cybercrime, they are still very popular. The attack is an attempt to crack passwords using mostly trial and error. In some cases, intensive computing processing is used to crack passwords, which also explains why it's called brute force. A well-known brute force attack was carried out on customers of Wordpress, a blogging platform, in 2013. Almost 60m brute force requests were carried out in one hour.

f) **SQL injection**: As the name suggests, the attack mainly targets databases. Malicious code is used to bypass the traditional application security to extract information from databases. The attack is

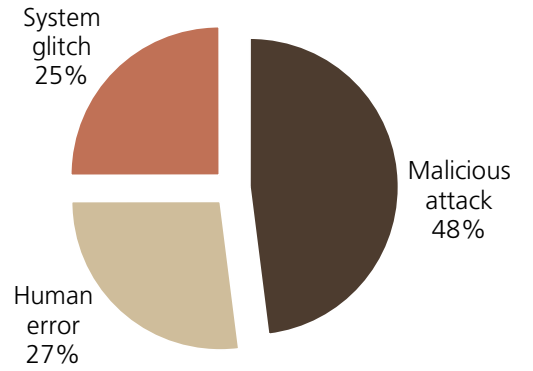
also meant to add, modify or delete records in the databases. Sony has been subject to SQL injection attacks in the past.

g) **Ransomware**: While ransomware is like any other malicious software (for example spyware), the difference lies in the way the users are locked out of their files or devices and are required to make a payment (i.e. pay a ransom) to restore access. The WannaCry ransomware attack in 2017 was one of the most well known, and was spread across almost 150 countries and industries.

How does it happen?

A study by the IBM Security and Ponemon Institute identified three major root causes behind data breaches. Malicious intent or criminal attack is the most common reason, accounting for 48% of the data breach incidents, followed by human error (27%) and system glitches (25%) (see Fig. 3). According to the study, the per capita cost of data breaches due to malicious attack was the highest at USD 157 followed by USD 131 for system glitches and USD 128 for human error. While the per capita cost for human error is the lowest, entrepreneurs should not underestimate it, as it's very difficult to track human errors until the attack is discovered. For instance, gullible employees may fall for phishing, use insecure passwords, or allow unauthorized users access to corporate devices which could result in major cyberattacks. As a result, we believe entrepreneurs should build a strong cyber security culture within their organizations which includes regular training. Entrepreneurs can also defend themselves from cyberattacks by reducing system glitches. This can be done by making sure IT infrastructure runs on the latest software that is less prone to security risks and avoiding application failures and logic errors.

Fig.3 Common reasons behind data breach



Source: IBM Security, Ponemon Institute LLC, (2018 Cost of a Data Breach Study: Global Overview), UBS

How your cyber approach can affect the valuation of your company

A company's value derives from its tangible and intangible assets. Intangible assets include not only patents, trademarks and copyrights but also a company's reputation and brand value. A study by Ocean Tomo (2015) shows that intangible assets have emerged as the leading determinant of a company's value. As shown in Fig. 4, in 2015 84% of the market value of the S&P 500 stemmed from intangible assets, while in 1975 this number was only 17%. The latter reflects not only the importance of integrating ESG (Environmental, Social, Governance) into a company's valuation but also how much more vulnerable its value is to reputational risks. This, together with the growing influence of social media and its ability to spread news and increase transparency, positions ESG risk and opportunity management as key to long-term sustainable value creation.

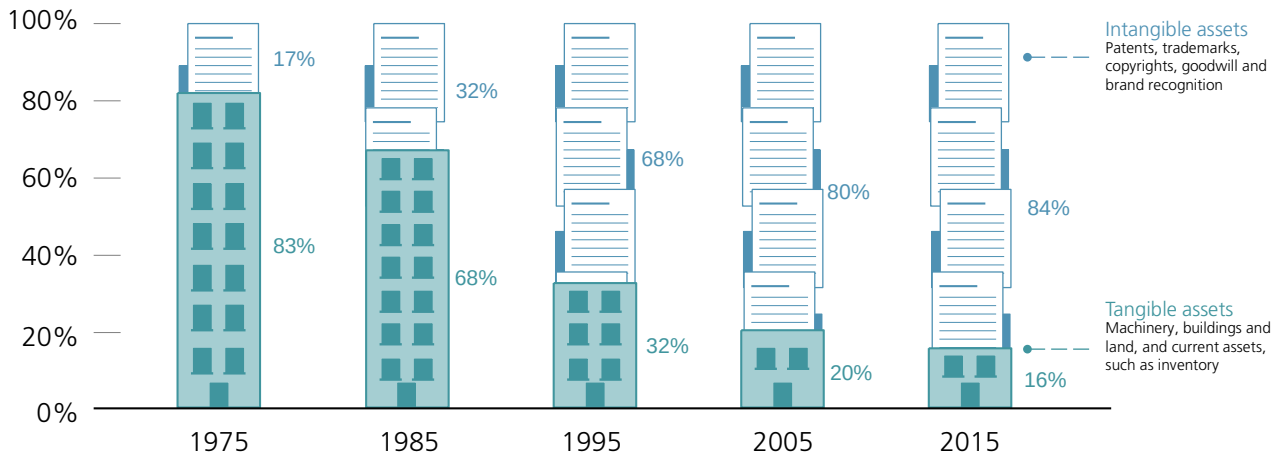
Customers vote with their wallets, and may not frequent companies with poor ESG criteria. Investors meanwhile vote with their capital and may not support or apply full value to companies perceived as being more risky or having poor sustainability criteria.

In our view, cybersecurity fits our sustainable investing framework given its key role in supporting the success of the Sustainable Development Goals (SDG). Cybersecurity is critical for technology to deliver progress effectively in a world that increasingly relies on computer systems. Supporting economic growth by preserving the benefits of digitalization can significantly contribute to SDG 1 – End Poverty. The 2017 a ransomware attack that shut down work across 16 hospitals in the UK greatly exemplifies the importance of cyber-

security to achieve SDG 3 – Good Health and Well Being. Mobile payment systems are increasingly important to achieve economic growth, cybersecurity hence plays a pivotal role in achieving SDG 8 – Decent Work and Economic Growth. Many other examples can be found on the overarching importance of robust cybersecurity frameworks to achieve the SDGs.

For companies, major risks derive from complying with new and more stringent regulations that can result in increased scrutiny and compliance costs. Leading companies will be those that have the right policies and organizational structures in place, invest in data security processes and adequately train employees on data security and privacy-related risks and procedures. Companies providing products and services that help enhance privacy features will be better positioned in an economy that no-longer supports business models that depend on violating individuals' privacy without their consent.

Fig. 4 Your cyber practices can affect the valuation of your company
Reputation is becoming more important in valuing companies. Intangible assets comprise the bulk of the market value for the S&P 500



Source: Ocean Tomo, UBS, as of 2015

This interview contains views which originate from outside Chief Investment Office Global Wealth Management (CIO GWM). It is therefore possible that the interview does not fully reflect the views of CIO GWM.

Interview with Crossword Cybersecurity

Stuart Jubb
Managing Director - Consulting, of Crossword Cybersecurity

Crossword Cybersecurity is a Technology Commercialisation company, solely focussed on Cybersecurity. We interviewed Stuart Jubb head of Consulting to understand some of the cyber issues entrepreneurs should think about in their businesses; and at what stage of the company lifecycle they should deal with them.

Q. Presumably companies can spend huge sums on cybersecurity. For a start up in particular this might be prohibitive. How do you suggest they go about it?
A. Absolutely costs need to be realistic and proportional to the business. Entrepreneurs will initially be focussed on developing a product and finding clients, however there are still some activities they can do, to reduce their cyber risks. We suggest different actions at different stages of a start ups lifecycle, for example:

- In the Pre product and start-up phase we suggest focussing on the basics such as Anti-Virus and security by design, where you apply the principles of confidentiality, integrity, and availability from the very start. This reduces the future potential vulnerabilities (weaknesses) that hackers will look to exploit. They should start thinking about additional technical controls such as encryption and vulnerability scanning. Getting Cyber Essentials[1] accreditation (or regional equivalent) is also recognised as a sound baseline of how secure your organisation is.
- In the growth and scale up 1 business phase, companies should look to build on the sound foundations and implement additional technical controls such as Multi Factor Authentication and carry out annual Penetration tests (ethical hacking). They should also start to consider Governance, Risk and Compliance controls such as a more comprehensive Information Security Policy, formal Governance and they may even have an Information Security Manager. They should also start to look at a more robust Governance standard, such as IASME[2]
- By the time companies reach the growth and scale up 2 phase, they probably have at least one FTSE100 (or equivalent) sized client who will have fairly stringent on-boarding procedures around cybersecurity. They will likely have a fairly mature set of cybersecurity controls and a culture which supports them. They may also have a suite of cybersecurity software products and a small cybersecurity team to support them. If budgets allow they will have a Chief Information Security Officer and be considering the ISO27001 accreditation.

Clearly all of the above is heavily dependent on the company's budget, and carrying out a thorough Risk Assessment/Management exercise and aligning this with the company's' business strategy. This will help companies prioritise where to spend their money.

Q. What security would you recommend a company have in place before it IPOs or gets acquired?
A. When looking to list what security a company should have in place before it IPOs, the answer is how long is a piece of string. However, they key thing is the for the Board to have a thorough understanding of where the Cybersecurity risks lie across the business and what their cybersecurity team are doing to manage and monitor those risks.

Most companies will carry out a Cyber Due Diligence on any company they are looking at acquiring, so keeping the above in mind, Executives should consider how their cybersecurity would look to an external party looking in. Getting an external advisor to do this can help here.

Q. How should a company decide how much of their cybersecurity to outsource and how much to keep in-house?
A. The best way to do this is to (a) carry out a Risk Assessment to understand the priority risks to the business; and then (b) carry out a Cybersecurity strategy. A cybersecurity strategy aligns the risks against the business strategy and then ensures the cybersecurity budget is spent in the most cost effective way. Too many companies just spend money on expensive software (and people) they do not really need.

Following this exercise, the company can then set the balance between in house and outsourced that best mitigates their cybersecurity risks and is the most efficient. As a general rule, the more that can be outsourced the better, within reason. This ensures that you have the most experienced people possible and it is also cheaper than bringing everything in house.

[1] Cyber Essentials (https://www.cyberessentials.ncsc.gov.uk/) is an accreditation through the National Cybersecurity Centre and helps you guard against the most common threats
[2] The IASME Governance Standard (https://www.iasme.co.uk/the-iasme-standard/) is an affordable and achievable alternative to the international standard, ISO27001, which builds on the foundations laid in Cyber Essentials.

Q. What are your thoughts on Cyber insurance? Is it an excuse for lack of proper cybersecurity or an essential for cyber aware companies?
A. I think it is helpful to have, assuming you understand what you are buying, but I would say a lot of companies tend to hide behind this and use it as an excuse. It is one small part of the solution and unfortunately, the reality is that companies really need to look at their culture, processes and technology and how they make them more secure. Cyber Insurance is not the answer in isolation.

Q. Thank you for your interesting insights, any last suggestions, advice or comments?
A. The area that I do not think companies are focussing on enough is Third Party Risk. There have been two recent fines by the Information Commissioners Office (ICO)[3] which were due to a supplier or third party being breached (hacked). This doesn't even take into account compensation from potential civil cases. We have found that criminals are increasingly targeting companies' supply chains and third parties, and I believe companies have a lot of work to do to improve the risks in these areas.

[3] https://ico.org.uk/

Ten tips for keeping your business cyber secure
There is always a balance to be had between keeping good security and efficient functionality. However, here are some basic steps all companies should take:

- **Staff training:** regularly train staff on cyber risk and good cyber hygiene, especially new joiners. In particular pay attention to phishing emails and provide tips on how to spot them, and make them easy to report. Training should also focus on the different examples of hacking including "mimicking" people they know both professionally and personally. Teach staff how to be cyber safe at home as well, as good practice will carry into work. For example use one email for personal banking, use another email for friends and family, and use a third email for marketing/shopping; include social media training for personal and professional use.
- **Device security:** Keep devices, software and apps up to date and limit access only to those people necessary. Ensure all devices are locked and have two factor authentication. Have everyone working on the same company devices, not their own – different set ups are harder to control. Be careful taking mobile phones abroad to sensitive countries. Do not use devices on insecure wifi networks (e.g. coffee shops). If a device is stolen make sure you can wipe it remotely. Prevent the use of USB sticks and other devices you can plug in unless they have had authentication – accidental errors or rogue employees/ vendors can download data or upload malware. Where smart devices are part of the operational processes (Internet of Things) such as in manufacturing industries, pay particular attention to the security of the IoT devices, which are often weak links.
- **Password security:** Use randomly generated passwords – don't use simple things – they can be guessed. Use different passwords for different systems. Suggest employees use different passwords at work than they do personally. Do not leave passwords on post it notes. Use 2 factor authentication when necessary. Change default passwords (e.g. on wifi systems or devices when they arrive). To enable staff to manage their pass-

words, consider password managers and ways to reset passwords if they are forgotten.

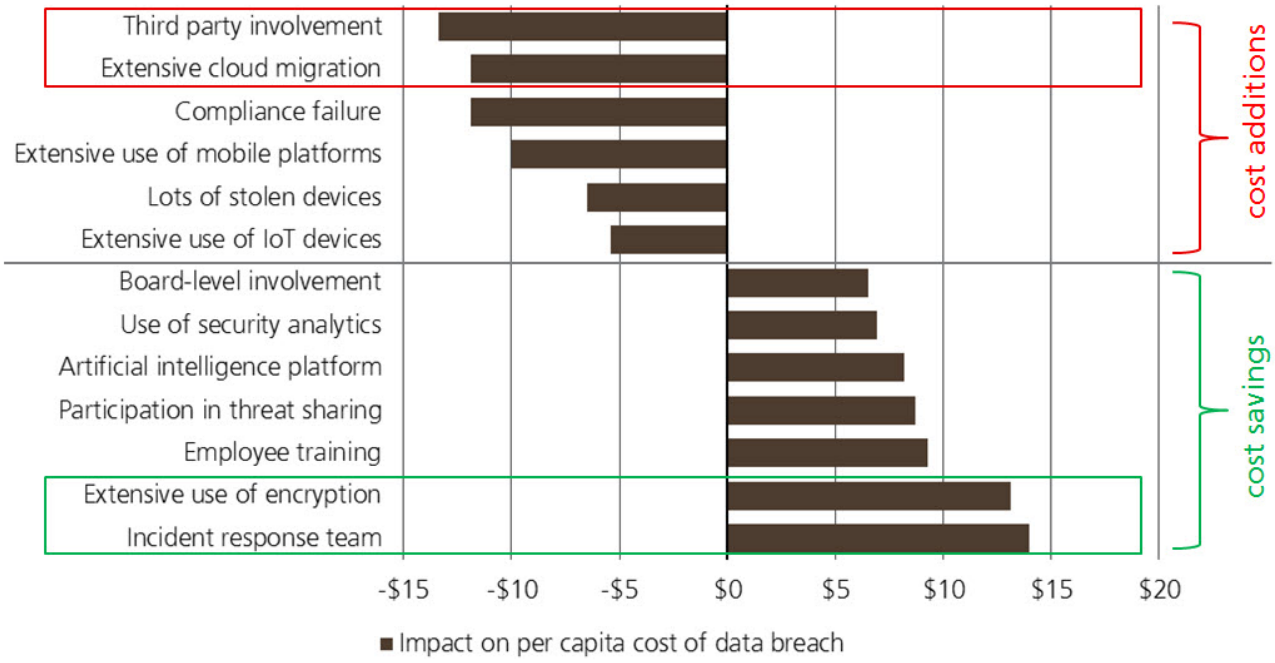
- **Keep software up to date:** Keep all software up to date, especially antivirus software, and don't overlook device and server software. And lock down servers and internet access. Be careful of some video conferencing facilities which are not fully secure and can be hacked. Limit access to software and programmes only to those necessary.
- **Security of data:** Keep client and employee personal data separate from other company data – GDPR is an important legislation with serious consequences and hefty fines for breaches. Decide which data needs to be backed-up and back up systematically. Limit the number of people who have access to the backed-up data. Decide which data needs to be encrypted – all data in a data center and back-up system should be encrypted. The cloud is usually quite secure, but most breaches occur at the access points – so ensure these are totally secure.
- **Chief Information Security Officer:** Appoint a CISO to be head of your cybersecurity. Clearly they need to work closely with IT, but they also need to have independence to challenge the IT security. Again it's a question of functionality (IT) versus security (CISO). They should create a good cybersecurity culture and ensure the whole company practices good cyber hygiene. Make sure cybersecurity is on your board's agenda and the CISO provides regular updates.
- **Cyber resilience plan:** Have a detailed plan and actions of how your company is staying cyber safe and constantly evolving to the latest regulations and latest threats. Be aware of the regulations for your particular industry but also keep ahead of the regulations to keep your company safest. A resilience plan will include regular monitoring; testing and penetration exercises. Don't forget to pay attention to companies in your supply chain or companies that may be acquired – proper cyber due diligence should be carried out before integration. If you are global, have a good information exchange across jurisdictions, so that if there is an attack in one area, the others can be alert to preventing it in theirs.
- **Cyber attack recovery plan:** Have a detailed plan of how to deal with, report to the regulator, and recover from a cyber attack. It's a question of when not if. This will include your cybersecurity advisers/vendors, your legal advisers, your regulator, your PR team, and the board.
- **Obtain a Cybersecurity rating:** Reassure yourselves, your investors, and your customers that you have good cyber practices, and are cyber mature, by obtaining a cybersecurity rating from a recognized body.
- **Cyber insurance:** Insurance is not an alternative to good cybersecurity, but it may be helpful in case of an attack. You don't want concerns about cost restraints to be a limiting factor when responding to an attack.

How to limit the cost of the impacts?

Based on research by IBM Security and the Ponemon Institute (see Fig. 5) there are certain factors that impact the cost of data breach in a positive but also negative way. The average cost globally for companies per individual stolen record is USD 148. Incident

response teams and the extensive use of encryption result in the greatest decrease in the cost per compromised record. On the other side, if third parties are involved costs might rise more than USD 10 per record, but investing in an extensive cloud migration could be a costly exercise. The background is that companies with cloud migration may be too focused on the migration, i.e. the IT department is absorbed with this project, while management might be focused on cost cutting as a result of the cloud migration (more details in the paragraphs below).

Fig. 5: Factors that impact the cost of data breach



Source: IBM Security, Ponemon Institute LLC, (2018 Cost of a Data Breach Study: Global Overview), UBS

How to increase detection rates

One major challenge for companies is that hackers can enter a system and steal data within minutes. Unfortunately, IT departments might discover the breach only much later, and it can take a considerable amount of time to contain it. A case in point was the Marriott data breach. The hotel group announced in late November 2018 that someone had hacked up to half a billion accounts (the latest number is 339 million). Hackers had entered the Starwood system (part of the Marriott group) in 2014. One of the pain points that firms face is the high number of (false) alerts that IT departments have to handle. Just hiring more people is not a long-term solution, as a good proportion of security spending already goes into people and processes and not software. Unusual network activity, including spikes in network traffic or a reduction in internet speed, sometimes coincides with cyber security breaches. This is another way to identify cybercrime detection rates. Increasingly, AI and machine-learning tools are being deployed, and we encourage entrepreneurs to embrace these given the high cost of cybercrime if not detected at an early stage.

Key words: cloud, IoT, and 5G – what is their impact from security perspective?

Cloud: Over the last few years, there has been an intense discussion about whether it makes more sense to keep an on-premise IT infrastructure for security reasons or to move everything onto the cloud. We think there is a broad consensus toward the latter. It is cheaper as firms save costs on datacentres, servers, network, heating and cooling, overheads, etc. In addition, many firms also use the cloud to benefit from the rapid innovation in this field. Cloud operators are much more innovative and invest more than businesses would typically invest in their IT infrastructure. Big hyperscalers and cloud operators such as Amazon Web Services or Microsoft Azure (market leaders) are responsible for the security of the cloud infrastructure. For their customers this means identity and access management. Encryption (of data in transfer) will become more important, to control who has access to data in the cloud, so as to avoid blindspots which allow cyberattacks.

Internet of Things (IoT): As a vast range of devices can be connected to the internet, the IoT will be a game-changer in terms of connected machines worldwide. This will create a big technology challenge for society and companies. For example, consider connected automobiles or planes in the future. If these are hacked this creates a more serious threat than the hacking of a smart phone. For private individuals as well as for corporate IT departments, it will become more complicated to protect all devices. We are currently seeing a broad variety and rising number of connected devices that companies have to control. It starts with your chip card to enter the building, the surveillance camera to protect your property, or the many connected robots and sensors in a factory, just to name a few examples. The number of attacks will increase and most people/ firms don't even know how their IoT devices are protected. When an electronics company develops a new camera, cybersecurity is not top of their mind. They want to develop an excellent camera that produces sharp pictures. But ask yourself, have you ever thought about how your smart lighting system, doorbell camera, or may be your smart smoke alarm is protected? Device visibility will be an important investment in terms of IoT and cyber security. If you don't know which device touches your corporate environment, how can you protect it? Cyber security experts believe a significant increase in attacks that involve IoT devices is likely. This is also reflected in the rising rate of growth in IoT security budgets (for more details please see our Security and Safety report, published in January 2019).

5G: 5G presents a lot of advantages for both consumers and companies. Most importantly it will have ten times more bandwidth than 4G and therefore is another driver of the IoT. Unfortunately, there are also security ramifications. It means firms have to control more devices of greater complexity, including likely autonomous vehicles and remote healthcare devices, with more IP traffic that needs to be inspected. All this leads unavoidably to more and potentially new cyber risks, patches, and more administration. On the positive side, 5G allows for increased encryption of data traffic and is subject to mutual authentication between device and network. This makes 5G technology more secure.

Threats to smart phones

How secure is your cell phone? To answer this question you have to consider how many phones are running on the newest major software version and best case also newest minor software version (patch). Based on statistics from Symantec (see Fig. 6), more than three-quarter of Apple phones (iOS software) were running the latest major software version in 2018, while Android users were more exposed to risk as less than one-quarter had the latest major software version. The statistics are worse for minor software updates. Only 30% of Apple phones had the latest version and only 5% of Android phones. It is important to make regular system updates to avoid leaks, for example of phone numbers, GPS data.

How to select the right cyber services companies to help you?

As with any vendor, it is a question of identifying your needs and budget, and interviewing a range of providers to see who most suits your needs.

Cyber services companies can provide a whole range of services, from consulting to training to monitoring and testing, as well as incident response. They can provide the security tools themselves, or you can provide them and give access to your cyber security vendor.

A recommendation from a trusted peer is one method of identifying a potential vendor for the shortlist. Additionally, most national cyber agencies will offer a range of recommended or accredited providers.

Conclusion

Cyber security ranks as one of the top three concerns for investors and business owners, and cyber security incidents are rising at 20%-30% per year. Globally, the average total cost of a data breach in 2018 stood at USD 3.86 million.

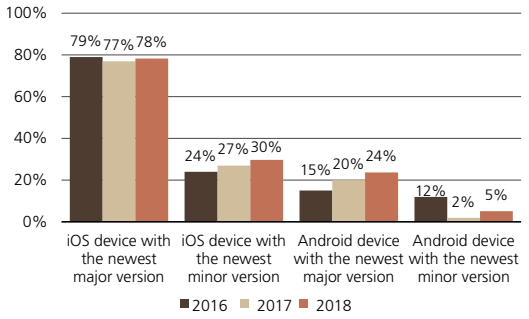
Small and medium sized enterprises are just as much at risk as the headline-grabbing larger companies.

There is always a balance between good security and efficient functionality. However, here are some basic steps all companies should take.

Ten top tips to keep your company cyber secure:

1. Staff training 2. Device security 3. Password security 4. Keep software up to date 5. Security of data 6. Chief Information Security Officer 7. Cyber resilience plan 8. Cyber attack recovery plan 9. Obtain a cyber security rating 10. Cyber insurance.

Fig. 6: Threats on smart phones



Source: Symantec (Internet Security Threat Report Volume 23 and 24)

Bibliography

Crossword Cybersecurity: www.crosswordcybersecurity.com

Forbes.com https://www.forbes.com/sites/david-prosser/2019/04/17/cyber-criminals-target-poorly-protected-small-businesses/#a456d1371776

IBM Security, Ponemon Institute LLC, (2018 Cost of a Data Breach Study: Global Overview), https://www.ibm.com/security/data-breach

Information Commissioners Office (UK regulator for reporting cyber breaches) www.ico.org.uk

Ocean Tomo Intangible Asset Market Value Study 2015

Symantec (Internet Security Threat Report Volume 23 and 24), https://www.symantec.com/blogs/threat-intelligence/istr-23-cyber-security-threat-landscape; https://www.symantec.com/blogs/threat-intelligence/istr-24-cyber-security-threat-landscape

The National Cybersecurity Centre www.ncsc.gov.uk

UBS Investor Sentiment 2Q 19. UBS surveyed 3,653 investors and business owners with at least USD 1m in investable assets (for investors) or at least USD 250k in annual revenue and at least one employee other than themselves (for business owners), from March 10–28, 2019. The global sample was split across 17 markets: Brazil, China, Germany, Hong Kong, Indonesia, Italy, Japan, Malaysia, Mexico, Philippines, Singapore, Switzerland, Taiwan, Thailand, the UAE, the UK and the US.

Appendix

UBS Chief Investment Office's ("CIO") investment views are prepared and published by the Global Wealth Management business of UBS Switzerland AG (regulated by FINMA in Switzerland) or its affiliates ("UBS").

The investment views have been prepared in accordance with legal requirements designed to promote the **independence of investment research.**
Generic investment research – Risk information:

This publication is **for your information only** and is not intended as an offer, or a solicitation of an offer, to buy or sell any investment or other specific product. The analysis contained herein does not constitute a personal recommendation or take into account the particular investment objectives, investment strategies, financial situation and needs of any specific recipient. It is based on numerous assumptions. Different assumptions could result in materially different results. Certain services and products are subject to legal restrictions and cannot be offered worldwide on an unrestricted basis and/or may not be eligible for sale to all investors. All information and opinions expressed in this document were obtained from sources believed to be reliable and in good faith, but no representation or warranty, express or implied, is made as to its accuracy or completeness (other than disclosures relating to UBS). All information and opinions as well as any forecasts, estimates and market prices indicated are current as of the date of this report, and are subject to change without notice. Opinions expressed herein may differ or be contrary to those expressed by other business areas or divisions of UBS as a result of using different assumptions and/or criteria.
In no circumstances may this document or any of the information (including any forecast, value, index or other calculated amount ("Values")) be used for any of the following purposes (i) valuation or accounting purposes; (ii) to determine the amounts due or payable, the price or the value of any financial instrument or financial contract; or (iii) to measure the performance of any financial instrument including, without limitation, for the purpose of tracking the return or performance of any Value or of defining the asset allocation of portfolio or of computing performance fees. By receiving this document and the information you will be deemed to represent and warrant to UBS that you will not use this document or otherwise rely on any of the information for any of the above purposes. UBS and any of its directors or employees may be entitled at any time to hold long or short positions in investment instruments referred to herein, carry out transactions involving relevant investment instruments in the capacity of principal or agent, or provide any other services or have officers, who serve as directors, either to/for the issuer, the investment instrument itself or to/for any company commercially or financially affiliated to such issuers. At any time, investment decisions (including whether to buy, sell or hold securities) made by UBS and its employees may differ from or be contrary to the opinions expressed in UBS research publications. Some investments may not be readily realizable since the market in the securities is illiquid and therefore valuing the investment and identifying the risk to which you are exposed may be difficult to quantify. UBS relies on information barriers to control the flow of information contained in one or more areas within UBS, into other areas, units, divisions or affiliates of UBS. Futures and options trading is not suitable for every investor as there is a substantial risk of loss, and losses in excess of an initial investment may occur. Past performance of an investment is no guarantee for its future performance. Additional information will be made available upon request. Some investments may be subject to sudden and large falls in value and on realization you may receive back less than you invested or may be required to pay more. Changes in foreign exchange rates may have an adverse effect on the price, value or income of an investment. The analyst(s) responsible for the preparation of this report may interact with trading desk personnel, sales personnel and other constituencies for the purpose of gathering, synthesizing and interpreting market information. Tax treatment depends on the individual circumstances and may be subject to change in the future. UBS does not provide legal or tax advice and makes no representations as to the tax treatment of assets or the investment returns thereon both in general or with reference to specific client's circumstances and needs. We are of necessity unable to take into account the particular investment objectives, financial situation and needs of our individual clients and we would recommend that you take financial and/or tax advice as to the implications (including tax) of investing in any of the products mentioned herein.
This material may not be reproduced or copies circulated without prior authority of UBS. Unless otherwise agreed in writing UBS expressly prohibits the distribution and transfer of this material to third parties for any reason. UBS accepts no liability whatsoever for any claims or lawsuits from any third parties arising from the use or distribution of this material. This report is for distribution only under such circumstances as may be permitted by applicable law. For information on the ways in which CIO manages conflicts and maintains independence of its investment views and publication offering, and research and rating methodologies, please visit www.ubs.com/research. Additional information on the relevant authors of this publication and other CIO publication(s) referenced in this report; and copies of any past reports on this topic; are available upon request from your client advisor.
Important Information about Sustainable Investing Strategies: Incorporating environmental, social and governance (ESG) factors or Sustainable Investing considerations may inhibit the portfolio manager's ability to participate in certain investment opportunities that otherwise would be consistent with its investment objective and other principal investment strategies. The returns on a portfolio consisting primarily of ESG or sustainable investments may be lower than a portfolio where such factors are not considered by the portfolio manager. Because sustainability criteria can exclude some investments, investors may not be able to take advantage of the same opportunities or market trends as investors that do not use such criteria. Companies may not necessarily meet high performance standards on all aspects of ESG or sustainable investing issues; there is also no guarantee that any company will meet expectations in connection with corporate responsibility, sustainability, and/or impact performance.
Distributed to US persons by UBS Financial Services Inc. or UBS Securities LLC, subsidiaries of UBS AG. UBS Switzerland AG, UBS Europe SE, UBS Bank, S.A., UBS Brasil Administradora de Valores Mobiliarios Ltda, UBS Asesores Mexico, S.A. de C.V., UBS Securities Japan Co., Ltd, UBS Wealth Management Israel Ltd and UBS Menkul Degerler AS are affiliates of UBS AG. UBS Financial Services Incorporated of Puerto Rico is a subsidiary of UBS Financial Services Inc. **UBS Financial Services Inc. accepts responsibility for the content of a report prepared by a non-US affiliate when it distributes reports to US persons. All transactions by a US person in the securities mentioned in this report should be effected through a US-registered broker dealer affiliated with UBS, and not through a non-US affiliate. The contents of this report have not been and will not be approved by any securities or investment authority in the United States or elsewhere. UBS Financial Services Inc. is not acting as a municipal advisor to any municipal entity or obligated person within the meaning of Section 15B of the Securities Exchange Act (the "Municipal Advisor Rule") and the opinions or views contained herein are not intended to be, and do not constitute, advice within the meaning of the Municipal Advisor Rule.**

External Asset Managers / External Financial Consultants: In case this research or publication is provided to an External Asset Manager or an External Financial Consultant, UBS expressly prohibits that it is redistributed by the External Asset Manager or the External Financial Consultant and is made available to their clients and/or third parties.For country disclosures, click here.
Version 05/2019. CIO82652744