COMMERCIAL BANKING

The financial impacts of a cyber attack

What cyber means for your environmental, social & governance strategy

BANK OF SCOTLAND

Contents

Executive Summary

1

This report provides an overview of the cyber threats that affect multiple industries and highlights the potential financial impact of a cyber incident.

2

COVID-19 has accelerated the pace of digital transformation for many companies and their reliance on technology. Cyber is a key operational risk with the potential for significant disruption to a business, its customers, brand, reputation and ultimately financial position. Cyber risk is increasingly becoming a key factor within the Environment, Social and Governance (ESG) considerations of a business's credit rating.

3

Malicious cyber actors pose a highly capable, persistent and growing threat to a broad range of industries. The cost of these threats continues to grow and operational disruption is often major: the combination can be fatal for companies.

4

Destructive malware has the potential to cause the greatest financial and operational impact.

5

Hybrid-Ransomware attacks have increased significantly in 2020. Attacks often involve bulk-data theft and wiper malware damaging company networks and operations. Victims incur high costs due to large ransoms – and subsequent regulatory fines.

Recommendations

- Organisations need to be aware of the dangers posed by leaving their systems and processes vulnerable to cyber attacks and put in place ways to prevent and minimise the impact of attacks.
- To create robust defences, a proactive response is required - matched with a high-level understanding of the latest cyber threat intelligence.
- Strong governance is essential. Companies need to make sure, both internally and across their supply chain, that required standards and security are met, processes remain up to date and short cuts aren't taken. From passwords to company leavers, emails to failsafe systems, an organisation's cyber security is only as strong as its weakest link. To be effective security needs to be taken seriously at all levels of an organisation – shopfloor to board-level.
- Understand how your cyber risk posture may be impacting on the ESG elements of your company's credit rating.

Introduction

Giles Taylor

Head of Resilience & Cyber Risk, Data Services

> The next time you see a company's name in the news because of a successful cyber attack, imagine what it would do to your organisation if it was your brand there instead.

Organisations and cyber criminals are in a seemingly never-ending struggle. As businesses tighten security, strengthen firewalls and ramp up their virus detection capability, attackers evolve different ways to exploit weaknesses, new technologies and loopholes they have found. So, we have put together an overview of the cyber threat landscape affecting multiple industries to demonstrate the potential financial impact of a cyber-incident.

Cyber risk may not initially be front of mind when environmental, social and governance (ESG) issues are discussed at a company board meeting. However, depending on the sector involved, cyber risk has a varying and significant impact on ESG issues increasingly feeding in to your credit rating.

Social and governance implications

For many companies the environmental impacts of a cyber attack may be limited (with the notable exception of energy and chemical companies), but social and governance factors are clear to see. These include the potential customer harm that a successful cyber attack can inflict and the complex governance, risk and reputational management requirements from the board down. For companies to address these challenges it is imperative to have a comprehensive view of the potential cyber impacts on an organisation.

The next time you see a company's name in the news because of a cyber failure, imagine what it would do to your organisation if it was your brand there instead.

Financial costs

Investors and other stakeholders are becoming more focused on governance issues – and cyber oversight being key among them. The costs associated with cyber attacks are growing as they become more damaging and more frequent – simultaneously, increased regulation has resulted in large fines, and victims can also face third-party lawsuits.

New risks

The cyber threat to businesses is persistent, evolving and growing in capability. It's a question of when not if…

The COVID-19 global pandemic has provided new opportunities for those with bad intentions. Changes in working practices, with more home working, businesses stretched thin by being unable to operate or trade as normal and a new variety of ways to trick unsuspecting victims means organisations and their employees need to be ever careful.

To be able to understand where the vulnerabilities lie for your business you will need to grasp how the cyber attack landscape is changing so that your governance strategy can evolve to meet new challenges. Organisations need the foresight to implement effective preventative measures and invest in appropriate mitigation and response measures to protect their operations, clients, customers and colleagues, and financial resilience.

Can you afford not to be ready for cyber threats?

Why your business needs to act now

The cyber threat is persistent, growing and affects all industries. Every such threat has three faces:

- the intent of the malicious actor,
- their capability including the tools, tactics, techniques and procedures they use
- the opportunities available to them to exploit the weaknesses of their victim's systems and technologies.

An organisation can face its greatest threats when the three align in the hands of someone acting against them. Dangers can come from both outside and within your organisation.

Externally, criminals, hackers and rogue states are enhancing their technical capability, driven by the profitability of cyber-crime and the expanding opportunities for illicit cyber activity. Whether driven by money, mayhem or malice, the net result can be disastrous for the unprepared.

Internally, employees have wider access to sensitive data, are adapting to new ways of working and are increasingly targeted as the weak link in security layers.

More complex and interconnected systems present new opportunities and entry points for bad actors as technology becomes more sophisticated.

The cyber threat is continually evolving to keep up with changing technologies and to exploit weaknesses. Specifically, ransomware is flourishing, targeting organisations of all sizes, with larger ransoms demanded. Destructive malware is becoming more advanced and widely used. Cloud data breaches are seemingly common. The impact of cyber incidents is also growing with the global cost of damages expected to reach $6 trillion annually by 2021[i].

Organisations of all sizes, in a wide spectrum of industries, are potential targets[ii]. Undoubtedly there will be major incidents in the year ahead, with significant cost impacts for the affected companies, and for organisations within their supply chain that may also face collateral damage. The perpetrators of these incidents will range from lone individuals, to organised criminal groups and state-sponsored actors.

Cyber threats: top 10 targeted industries

Sector	2019 Rank	2018 Rank
Financial services	1	1
Retail	2	4
Transportation	3	2
Media	4	6
Professional services	5	3
Government	6	7
Education	7	9
Manufacturing	8	5
Energy	9	10

Source: IBM Security X-Force Threat Intelligence Index 2020

Ransomware

Ransomware targeting private and public organisations has grown dramatically as data has become more valuable. Organisations of all sizes and industries are targeted, with the most capable attackers targeting the largest companies and demanding the largest ransoms. The highest demand revealed so far is $42m[iii]. Ransomware attacks are now commonly used as a camouflage to steal data before scrambling networks into a secret code or freezing them to make them unusable. Often, part of the data is posted online and used to extort a ransom. Ransomware groups appear to be co-operating to improve their ability to profit from these attacks.

The cost of a ransomware attack can include:

- a ransom (if one is paid)
- the costs of remediation to networks and hardware
- lost revenue
- brand damage
- potential associated fines
- third-party claims.

In some circumstances, losing control of operating systems may represent a significant threat to life. In addition, losing the confidentiality of any stolen data results in its integrity being lost[iv].

Ransomware

Ransomware is a type of malware designed to coerce victims into paying a ransom, often by restricting access to a computer, device or files until the user pays a fee. But remember, paying the fee doesn't guarantee that the computer will be released so that you can regain access to your information and system. After all you are dealing with criminals.

Other times, messages asserting that they are from law enforcement agencies are displayed, claiming the user has been involved in illegal online activities, and providing instructions to pay a fine.

Average ransom demand costs

$600,000
Largest reported ransom paid in 2019

$84,116
Average ransom demand Q4 2019

$1,500
Commonly demanded from small businesses in 2019

Source: SPEC, Impact and Cost of Ransomware Attacks

Ransomware

The most common industries targeted by ransomware and the routes used

The most common way for a hacker to gain entry to target victims with ransomware is via a remote desktop protocol (RDP). RDP is a way of providing administrators, engineers and users with remote access to Windows operating systems. The protocol, which allows companies to fix and update their computers without someone having to be on the spot, can be exploited to plant ransomware from anywhere in the world. Those carrying out the attacks – threat actors – typically use credentials widely and cheaply available for sale online. The growth in working from home has magnified this risk further. Small and medium sized businesses account for the majority of this type of incident.

Phishing

Larger organisations are more likely to be targeted with phishing e-mails[v].

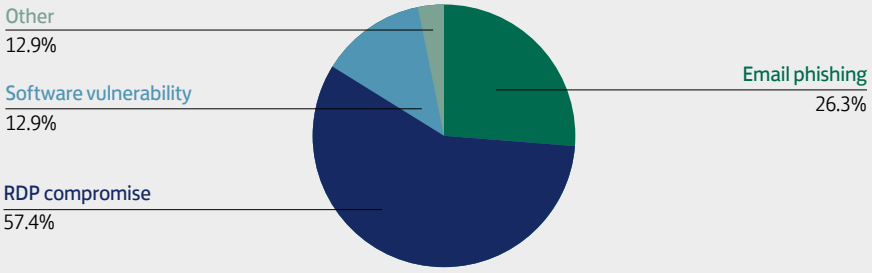
Phishing is where someone will try to obtain sensitive information from a victim by email. The sender will claim to be emailing from a trusted source, such as a colleague, the victim's bank or similar.

The email would typically direct the recipient to a website which will ask them to share their passwords, credit card details, personal information or alternatively can install malware on the victim's device.

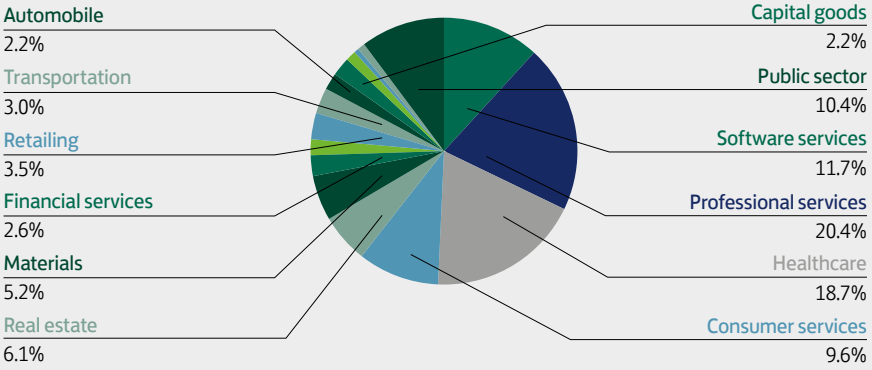
Professional services and healthcare were the two most commonly targeted sectors for ransomware attacks. The threat to the healthcare sector is likely to have grown in 2020, with the industry already stretched thin by the COVID-19 pandemic. The US Joint Cybersecurity Advisory updated its alert on ransomware targeting healthcare in October 2020 warning of new threats.

Hospitals clearly face real pressure to access records quickly, which puts pressure on them to pay any ransom fast – making them a tempting target. The volume and type of client records in professional services is an obvious draw in this sector. But all businesses face risks and even those in less-frequently targeted sectors still need to be alert to the hazards.

Most common ransomware attack vectors Q4 2019



Industries most targeted by ransomware Q4 2019



Source: Coveware Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate

Ransomware: emerging trends and threats

Ransomware is proving itself as a profitable business model for malicious actors. For that reason, it is highly likely to become more prevalent, and so increasingly sophisticated. Threat actors will increasingly steal data to aid in securing a ransom and providing additional revenue streams.
The cost impact for victims will grow as ransomware becomes increasingly frequent and sophisticated, stealing more data and deploying destructive tools.

Source: SPEC, Impact and Cost of Ransomware Attacks

Destructive attacks and Distributed Denial of Service (DDoS)

Destructive attacks, including ransomware attacks, which involve making the victim's data, software or hardware unusable, are increasing both in speed and scale. The average cost of a destructive attack to the victim organisation is $239m[vi].

Destructive attacks are frequently linked to hostile state actors - foreign governments and their supporters - motivated by wider geo-political drivers, from stealing secrets to covert warfare. As a result, industries and organisations central to national interests or critical national infrastructure are more likely to be targeted. However, these types of attacks have the potential to cause widespread and unintended damage beyond the intended target. This was dramatically seen in the 2017 NotPetya[vii] malware campaign, which saw companies and organisations like the NHS across the globe affected. While NotPetya is part of the Petya ransomware family, it is different from most ransomware as it cannot decrypt itself and return the computer system to how it was before the infection. Therefore, it is considered highly destructive malware.

Destructive malware

Criminal groups wanting to cover their tracks are embedding the use of destructive malware into their operations. This is typically done after access is gained to a victim organisation's network. It is designed to make it easier to avoid detection and harder to identify the perpetrators. Any subsequent damage caused by this activity adds to both the financial and operational impact of the primary cyber-attack.

DDoS attacks are highly prevalent and target a variety of industries, in particular: gaming, internet & telecommunications, financial services and media & entertainment.

DDos impact

Conducting DDoS attacks is relatively easy, with services widely available for sale online. The power and complexity of these attacks are also increasing[viii]. The longest uninterrupted DDoS attack in 2019 lasted three days, 13 hours and eight minutes[ix].

The impact from a DDoS attack on a target's services can last for the duration of an attack or fluctuate in line with the amount of traffic targeting the website. For example, customers may be unable to use a website for the whole time the attack lasts. Service impacts can also be felt after the attack because of the time it takes to get things back to normal. Increasing numbers of internet of things (IoT) devices, and the implementation and growth of 5G for mobile devices, will enable larger and more complex DDoS attacks resulting in greater impacts[x].

Financial losses resulting from NotPetya cyber attacks

$870m: Mereck (Pharmaceuticals)

$400m: FedEx (Shipping & Delivery)

$384m: Saint-Gobain (Construction)

$300m: Maersk (Shipping)

$188m: Mondelez (Food & Beverage)

Source: Coveware, Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate

Distributed Denial-of-Service

A DDoS attack is when large amounts of bogus traffic is channelled to a website, server or network with the aim of overwhelming the target causing it to crash and prevent genuine users from accessing services.

DDoS attacks are hard to mitigate as the malicious traffic originates from many distributed devices.

Destructive attacks & DDoS: emerging trends and threats

State actors will increasingly use destructive cyber attacks as a tool in geo-political and military disputes. Monitoring geo-political tensions may offer indicators of a rising threat. Malicious criminal actors will also increasingly incorporate destructive capabilities into their attacks. Therefore, future attacks are more likely to result in greater damage and recovery costs than previously.

The increasing capability of DDoS attacks will result in higher cost impacts for victims, too.

Insider threats and data breaches

More and more companies are using data and customer intelligence to help them improve service and forge their strategy, resulting in rapidly expanding pools of information. Employees have greater access to these growing data sets increasing the potential of an intentional insider incident, or an accidental data breach. In addition, hostile actors have been seen attempting to recruit insiders from various industry sectors.

The threat trajectory indicates that potential financial harms to victims from insider threats are rapidly increasing:

- Over the last two years, insider incidents have risen 47%[xi].
- Costs arising from insider threats have risen 31% in two years, to an average of $11.45m[xii].
- An intentionally malicious data breach typically costs three times that of an accidental one[xiii].
- 90% of data breaches are caused by human error[xiv].

The repercussions of data breaches are also growing with increased regulation. The General Data Protection Regulation (GDPR), enshrined within the UK's Data Protection Act (2018), enables regulatory fines up to €20m or 4% of annual turnover – whichever is highest.

Cloud services have become an epicentre of data loss incidents. The pooled data sets they hold make them an attractive target to malicious actors. Misconfigurations and unintentional errors that do the cyber equivalent of leaving a door open are more common than successful attacks, but still expose huge amounts of records in one incident. Reasons identified for the scale and frequency of such incidents include:

- inexperienced users
- complex and outdated security models
- a lack of unified cloud visibility
- the rate of change.

Impacts from cloud misconfigurations

>33bn: records accidentally exposed by cloud misconfigurations. 2018-2019

$5tr: estimated worldwide cost of Cloud misconfiguration breaches. 2018-2019

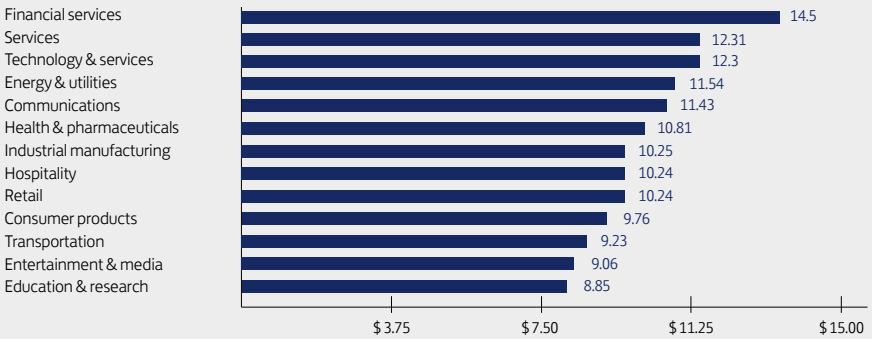
99%: of misconfigurations are the fault of the customer

Source: Tech Republic, [20 February 2020]

Insider threat and data breach: emerging trends and threats

Malicious and negligent data loss incidents are likely to grow in size and frequency as organisations collect, store and share data online in greater volumes. The transition to Cloud services will be a significant factor in the number of incidents occurring and organisations should carefully plan and manage the transition to reduce the risk. Cloud services will be heavily targeted by malicious actors. Remediation, 3rd party lawsuits and regulatory fines significantly increase the costs associated with a data breaches.

The annualised costs of insider activity in the USA by sector



Source: Ponemon Institute, 2020 Cost of Insider Threats Global Report

Supply chains

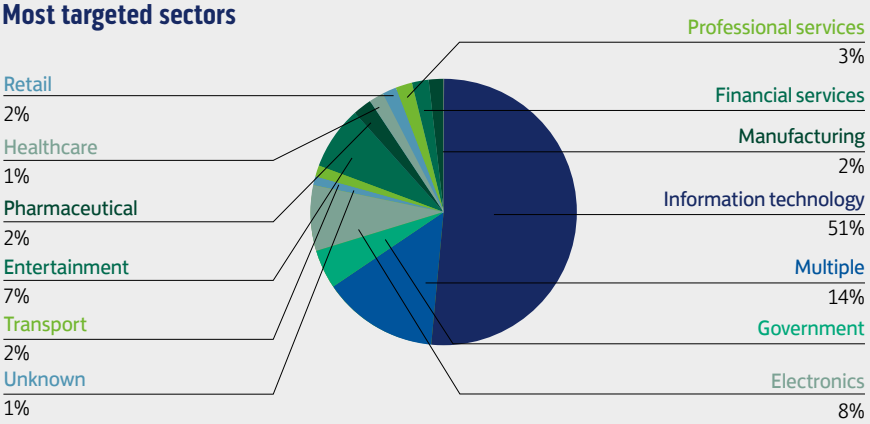
Access creep
Also known as privilege creep, this is the slow accumulation of unnecessary permissions, access rights, and outright privileges by individual users. This may occur as employees move jobs or projects and retain permissions and access rights they no longer need.

The supply chain frequently represents the greatest vulnerability to an organisation[xv]. All industries are a potential target. Suppliers frequently hold data belonging to their clients and have access to their networks. But suppliers are often not as well defended as the organisations they serve. Putting in place systems to oversee and provide reassurance about their controls is also difficult. Attackers look to exploit suppliers' relative vulnerability for financial gain and the chance to snoop around systems for other potential opportunities.

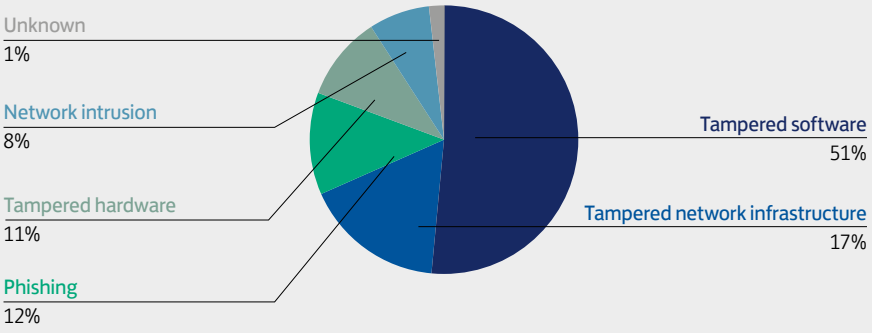
Many attackers look to use a supplier's network access to across to other, connected targets. In the cyber world this is known as an island hop where one network is used to jump across and gain access to a second. A study in 2019 showed that 50% of cyber-attacks use island hopping[xvi].

Suppliers that hold the most data, or have the most integration with their clients' systems, are likely to be the most targeted. Limiting the data and access suppliers hold can reduce the dangers, as would audits to stop 'access creep' occurring. It is important that companies follow strict movers and leavers processes in order to avoid this.

Most targeted sectors



Most common threat methods



Source: Open Source research of 101 supply chain incidents [April 2015 – April 2020]

Supply chain: emerging trends and threats

Targeting suppliers for their clients' data and access is highly likely to increase. This will result in significant cost impacts to the supplier and their clients. Operational impacts will also be felt where suppliers are unable to offer their services while they recover.

Advancing technology threats

A number of significant developments in technology have the potential to increase the reach and impact of cyber incidents.

Artificial Intelligence (AI)

AI is most likely to be used for data analysis rather than directly weaponised, at the moment[xvii]. AI could enable attackers with existing access to networks to better personalise falsified communications, making it more likely that users will click on malicious links or attachments.

AI will give attackers better understanding of user behaviour to identify the most valuable targets within a network[xviii]. As AI advances, Deep Fakes will become more realistic and malicious programs will be able to automate social engineering and impersonate live chats, such as with IT support or colleagues.

Internet of Things (IoT)

An estimated 20bn IoT devices ranging from smart lightbulbs and security cameras to engines that report back on their state of repair will be in use by 2021[xix]. But they are often vulnerable due to default passwords, outdated software and unencrypted traffic[xx]. They will be increasingly exploited as an initial entry point and from there to gain access to other points in the system.

By their very nature, it can be easy to put this type of device in place and forget about it, without applying the same rigorous password, patching and tracking rules within an organisation as more obviously vulnerable assets such as computers and servers do.

IoT devices typically have weak security measures making them ideal targets for creating a botnet (a network of internet-connected devices controlled remotely by a user). Malicious actors exploit this to drive large amounts of bogus traffic to a website making it crash in what is called a Distributed Denial of Service attack (DDoS).

Mobile devices

There is an increase in intercepting traffic on unsecured WiFi networks, sending ransomware and malware through SMS platforms or deployed through corrupted or malicious mobile apps. Staff need to understand the risks of using coffee shop or similar WiFi and of using their own devices on an organisation's network.

Apps containing malware or ransomware are developed using legitimate tools to evade detection and ensure they can be successfully uploaded to app stores, making them available to the mass market. Once loaded onto the device, ransomware extortions initiate or malware can run undetected[xxi]. Malware strains often steal personal identifiable information, contact details, login details and send and intercept messages – such as MFA (see below)[xxii].

Multi Factor Authentication (MFA)

This is a security process that requires users to present more than one credential to access a system or account, such as a password and a code sent to a registered phone or fingerprint to verify identity. It's also sometimes known as 2FA (two factor authentication).

As MFA usage rises, attackers will increasingly innovate to overcome it. Many MFA systems allow the same contact details to be used for authentication and password re-set. This allows attackers to re-set a password using stolen contact details, without ever having to know the original password. As a result, it is likely that databases of contact details will be increasingly targeted given their value to enable onward exploitation.

In addition, attackers will look to target system operating controls in order to gain admin rights allowing them to change authentication details and self-authenticate[xxiii].

Conclusion

Every organisation faces a live, complex and fast-evolving cyber threat, across a range of techniques as we have outlined here.

Leaders need to take their ESG responsibilities seriously and – in the case of cyber – focus on governance. Company boards need to be sure their organisation's most important information is being properly secured and managed. A failure to grasp the serious nature of the cyber threat currently being faced could be fatal for some organisations.

As we have seen with the growth of green reporting resulting from customer demand and regulators, a parallel pressure is arising around cyber attack issues. In future, some companies may need to provide more transparency about their cyber readiness and resilience. Investors and other key stakeholders will want to reassure themselves that the business is resilient enough to survive and thrive if hit by a cyber attack or shock of some sort. As business and society becomes more digital the greater the imperative to be ready to deal with cyber threats.

Impacts span reputational damage to major operational disruption, incurring substantial costs and in some instances causing businesses to go under. It is essential that companies strive to understand their exposure to the cyber threat landscape and invest the time, resource and expertise to effectively mitigate the threats they face now – and in the future. Governance and social responsibility are at the heart of dealing with a cyber threat.

What to do next

How should you report a cyber attack?

If your business, charity or organisation is under attack, if you have cyber insurance cover contact your insurer first, then consider reporting and seeking support from ActionFraud or call them on 0300 123 2040. This service is available 24 hours a day, 7 days a week.

Where to get more help and information

- Download a copy of Bank of Scotland's Cyber Security Guidance
- Stay one step ahead of cyber risk
- What to do about dark web threats

Other useful resources

- 10 steps – Board Responsibilities
- Action Fraud
- Cyber Essentials
- Get Safe Online
- Stay Safe Online
- NCSC cyber security advice for small and medium sized organisations
- NCSC cyber security advice for large organisations
- The European Union Agency for Cybersecurity – Threat Landscape Report 2020

Sources

[i] Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021, Cyber Crime Magazine, [December 2018]

[ii] IBM Security X-Force Threat Intelligence Index 2020, [February 2020]

[iii] Ransomware gang asks $42m from NY law firm, threatens to leak dirt on Trump, [15 May 2020]

[iv] SPEC, Impact and Cost of Ransomware Attacks, [14 May 2020]

[v] Coveware, Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate

[vi] IBM, Combating Destructive Malware, [2020]

[vii] The Untold Story of NotPetya, the most devastating Cyberattack in History, [22 August 2018]

[viii] Akamai, Financial Services Attack Economy, [2019]

[ix] Help Net Security, Across-the-board increase in DDoS attacks of all sizes, [27 March 2020]

[x] IndusFace, DDoS Attack Trends To Watch in 2020, [17 December 2020]

[xi] Ponemon Institute, 2020 Cost of Insider Threats Global Report [2020]

[xii] as above

[xiii] as above

[xiv] KnowBe4, Most British Breaches Traced to Human Error, [11 February 2020]

[xv] Wired, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, [22 August 2018]

[xvi] Carbon Black, The Ominous Rise of "Island Hopping" & Counter Incident Response Continues, [April 2019]

[xvii] F-Secure, Artificial Intelligence Attacks [11 July 2019]

[xviii] World Economic Forum, 3 ways AI will change the nature of cyber attacks [19 June 2019]

[xix] Aria Cybersecurity Solutions, Five examples of IIoT/IoT Security Threats [07 February 2020]

[xx] Paloalto Networks, 2020 Unit 42 IoT Threat Report [10 March 2020]

[xxi] McAfee, Mobile Threat Report [2020]

[xxii] Trend Micro, Mobile Banking Trojan FakeToken Resurfaces, Sends Offensive Messages Overseas from Victims' Accounts [16 January 2020]

[xxiii] Flashpoint, SIM Swappers Employ Variety of Account Takeover Techniques Following Phone Number Theft. [01 March 2020]

Find out more

Go to www.bankofscotland.co.uk/business

Please contact us if you would like this information in an alternative format such as Braille, large print or audio.

Our service promise

If you experience a problem, we will always try to resolve it as quickly as possible. Please bring it to the attention of any member of staff. Our complaints procedures are published at business.bankofscotland.co.uk/business-home/contact-us.html

Important information

While all reasonable care has been taken to ensure that the information provided is correct, no liability is accepted by Bank of Scotland for any loss or damage caused to any person relying on any statement or omission. This is for information only and should not be relied upon as offering advice for any set of circumstances. Specific advice should always be sought in each instance.

Any views, opinions or forecasts expressed in this document represent views or opinions of forum participants and are not intended to be, and should not be viewed as advice or a recommendation from Bank of Scotland or any other party.

Bank of Scotland plc Registered Office: The Mound, Edinburgh EH1 1YZ. Registered in Scotland no. SC327000. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority under Registration Number 169628.

BANK OF SCOTLAND