qLegal

The small print for BIG IDEAS

Disclaimer: This online publication describes the law in general terms. It is not intended to provide legal advice on specific situations and should not be relied upon as a source of legal advice.

Date produced: 8 April 2021

qLegal Online Publication

Protecting your start-up from a cyberattack

This online publication explains how a start-up can protect itself from a cyberattack.

Protecting your start-up from a cyberattack is an essential part in ensuring its success. Start-ups are easy targets due to the common misconception that they have nothing to offer cybercriminals and not spending enough time and resources on cybersecurity measures. This toolkit identifies key cybersecurity challenges for start-ups, the laws and regulations that you must comply with and the policies and procedures that you should put in place to prevent and deal with cyberattacks. It also provides practical solutions to securing your network to conduct business.

WHAT IS A CYBERATTACK?

A cyberattack involves directly targeting a business and weak cybersecurity infrastructure to disrupt, destroy, disable or gain access to data using a variety of methods.

HOW DOES IT AFFECT MY BUSINESS?

Start-ups are increasingly reliant on digital technologies and the internet to conduct their business and store data. It is necessary to understand how to protect your start-up and implement proper precautions and procedures to shield your business from cyberattacks and to comply with the relevant cybersecurity laws. Failing to comply with the rules can result in heavy penalties as well as damage to your reputation and loss of business.

43% OF CYBERATTACKS TARGET START-UPS

VERIZON DATA BREACH REPORT, 2019

HUMAN ERROR IS A MAJOR FACTOR IN CYBERATTACKS

GALLAGHER, 2020

TYPES OF CYBERATTACKS

Malware: Short for malicious software, it is a blanket term for Trojans, viruses and other cyber tools used to gain access to a network, steal or destroy data and damage computer systems.

Ransomware: A type of malware attack where data is encrypted and inaccessible until a ransom is paid.

Phishing: Cybercriminals send fake messages to convince victims to send sensitive information. They can contain faultless wording and official logos.

Whaling: Highly targeted spear phishing attacks aimed at senior executives, containing personalised information, conveying a sense of urgency and crafted with the business language and tone.

Hacking: Hackers gain unauthorised access to and control over computer systems or private networks through a targeted attack. They can steal or destroy information or prevent authorised users from accessing their own systems.

46% OF GLOBAL BUSINESES ENCOUNTERED AT LEAST ONE CYBERATTACK IN 2020* BARRACUDA, 2020	71% OF RANSOMWARE ATTACKS TARGETED SMALL BUSINESS WITH AN AVERAGE RANSOM OF $116,000 IN 2018** BEAZLEY BREACH RIEFING REPORT, 2019	90% OF BREACHES ARE PHISHING ATTACKS EXPERT INSIGHTS, 2021

THE IMPORTANCE OF CYBERSECURITY

Cybersecurity is the adoption of technical and organisational measures to prevent vulnerability to cyberattacks. Sound cybersecurity policies and procedures ensure that confidential and personal data of customer, partner, staff and any information relating to the business is secured and not made publicly available. Cybersecurity is important for a number of reasons:

- **Regulation and compliance** – cybersecurity and data protection laws require businesses to protect data. For example, the European Union's **Network and Information Security Directive 2016** and the European Union's **General Data Protection Regulation 2016 ("EU GDPR")** which have both implemented into the UK by way of the Network and Information Security Regulations 2018 and the UK GDPR 2020 (see below), place obligations on businesses**.**
-

- **Duty of care –** Start-ups have a responsibility to customers and partners to protect data and information**.**
- **Reputation –** Cybersecurity helps to protect the integrity of the business. Being vulnerable or falling victim to cyberattacks can shape customer perception and damage business reputation.
- **Financial –** Cyberattacks can result in significant financial losses, in terms of falling victim to these crimes and in penalties for failure to comply with relevant laws.

CYBERSECURITY IN 2020 – 2021

COVID-19, the global pandemic and the introduction of remote working introduced significant cybersecurity challenges for business. Cybercriminals have capitalised on remote working tools and platforms. Ransomware continues to be the fasted growing cybercrime and phishing attacks have adapted to exploit the remote working model by using themed attacks.

PREVENTATIVE MEASURES TO PROTECT AGAINST CYBERATTACKS

SECURE PASSWORD	TWO-FACTOR AUTHENTICATION	ANTIVIRUS SOFTWARE	BACKUP DATA	IDENTIFY PHISHING	TRAINING STAFF

Password safety: Create strong passwords that do not use easy to guess or personal data, such as your name or date of birth. Do not reuse passwords and change them often. If using a shared device, do not save the passwords to the device browsers.

Two-factor authentication ("2FA"): 2FA increases the security of your system by sending a one-time passcode to your email address or phone number.

Using the latest versions of software: Make sure that your business is using antivirus software and that it, and all other applications, are kept up to date on all devices used in connection with the business. If working with confidential information, use secure cloud services such as Dropbox or Google Docs instead of downloading the information locally to your device.

Backup data: This is a preventative measure, in the event of a loss of data or if your data is being held for ransom.

Identifying phishing: Phishing is becoming more sophisticated with faultless wording and official logos. Steps you can take include checking the actual email address or phone number of the sender of the email/text, as they are usually set up to appear from a known third party, such as your bank, but a closer look will show that the email address/number does not match who they claim to be. Also, never click on links from these suspicious emails or texts, as you run the risk of malware entering your system.

Training staff: Human error is one of the main factors that leads to a successful cyberattack. Ensure all staff receive adequate training on cybersecurity and how to not fall victim to cyberattacks such as phishing and social engineering.

LAWS AND REGULATIONS APPLICABLE TO BUSINESSES

EU GDPR and UK GDPR

The UK GDPR refers to the UK's version of the EU GDPR which has been amended and transposed into the UK law by way of the Data Protection Act 2018 and the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019.

The UK GDPR places businesses under an obligation to protect unauthorised or unlawful access to personal data by third parties. The Information Commissioner's Office (ICO) ensures compliance with the UK GDPR. If your business experiences certain types of data breaches, you must self-report to the ICO within 72 hours of becoming aware of the breach. Failure to do so may result in a fine. Customers or other "data subjects" (including your employees) may also file complaints with the ICO.

ICO Dawn Raids

Under the UK GDPR, the ICO's dawn raid powers were extended, allowing them to conduct dawn raid investigations on any UK business that controls or processes personal data. The ICO may enter a premise with a warrant. They usually give seven days' notice, but this may be reduced to zero days' notice where the ICO can show there are reasonable grounds for suspecting non-compliance with data protection legislation. Alongside any compliance failures discovered during the inspection, failure to comply with the execution of the warrant can lead to criminal and financial penalties.

Policies and procedures to prepare for and deal with ICO dawn raids

Being prepared for a dawn raid is key to reducing the risk of being taken by surprise and facing potentially significant criminal and financial penalties. The ICO has not published any specific guidance but steps to prepare for a dawn raid include:

- identifying a dawn raid response team with a leader and key senior figures in the business;
- ensuring all key employees are adequately trained on data protection and storage and what to do if there is a dawn raid;
- creating roles for each team member and document their roles and responsibilities;

- having a list of personnel who need to be informed in the case of a dawn raid (include their contact numbers and email addresses);
- practicing by conducting a mock raid; and
- training all staff on what to do and what their responsibilities are if they have to take part in interviews during a dawn raid. They may be liable criminally if they refuse to answer questions or if they provide false statements.

Network and Information Security Regulations 2018 ("NIS Regulations")

The NIS Regulations relate to the specific types of businesses such as such as cloud service providers and online marketplaces (e.g., data service providers). These businesses must implement "appropriate and proportionate" measures to minimise the risk and impact of attacks affecting the security of the network and system.

Failure to comply with requirements under the NIS Regulations may result in enforcement action and/or a fine. Similarly, businesses are required to notify the relevant competent authority within 72 hours of an incident.

HOW TO SAFELY USE ZOOM AND MICROSOFT TEAMS FOR YOUR BUSINESS

During the Covid-19 pandemic, we saw a huge increase in the use of these platforms by businesses working from home. This method of working will likely continue in 2021, and it may even become a permanent part of our working behaviour. As a result, it is important to know how to use these platforms safely. Below are some tips to implement while using Zoom, Microsoft Teams or any virtual meeting application:

- use the latest versions of the applications;
- secure your meetings with passwords and distribute them only to your intended attendees. The best way for companies to do this is by having access to a "single sign on" function;
- use "waiting rooms" as a way to screen those joining the meeting, so you can exclude anyone that was not invited;
- secure your internet connection to stop hackers by changing the router name and setting a strong password, turning on encryption, turning off the Wi-Fi Protected Set-Up ("WPS"); and
- avoid using a public network as they are not secure and for added protection, consider using a Virtual Private Network ("VPN").

OTHER ALTERNATIVE PLATFORMS FOR SAFE MEETINGS FOR START-UPS

Platforms that offer online meeting tools such as sharing presentations and scheduling meetings.	Zoho, Nextiva, Ring Central, Join.me, BlueJeans, Fuze, Jive Voice
Exclusive platforms that offer options of a one-time usage or the option of customising a brand while hosting a meeting or video conference. They can also be accessed through a desktop app.	Skype for business, Amazon Chime, Adobe Connect, Cisco
An app that offers cloud-based storage and can be used to make calls via a broadband connection.	Vonage
A cost-effective platform that can be used be used by start-up's, especially at an early stage of their business with all forms of collaboration.	FreeConferenceCall.com

CONCLUSION

The use of digital platforms has increased multi-fold over the last decade and recently due to the global pandemic, most start-ups have had to move their businesses online. They can save themselves from being targets of cyberattacks, phishing and hacking by following simple methods and procedures of safety, while using online platforms or databases. With the growing importance of data protection, businesses are now under legal obligations to comply with certain laws and potentially face huge criminal and financial penalties if they do not comply.

This online publication was drafted by students from the Centre for Commercial Law Studies, Queen Mary University of London: Bibi Fathema Rahman, Jahnavi Murthy Mocherla, Zoe Asser.