MOORE Kingston Smith
GDPR Data Protection Solutions
POWERED BY ClearComm

# CHALLENGING COMPLACENCY
# IS YOUR TECH COMPANY AT RISK?

The government's Cyber Security Breaches Survey 2020 indicates that cyberattacks have evolved and become more frequent.[1] Almost half of businesses surveyed reported breaches or attacks in the 12 months prior to the survey, with 32% of affected businesses claiming at least one incident per week. On the last day of September, and as a response to the spike in cyber-attacks since June the National Cyber Security Centre posted "Doing nothing is no longer an option – raise your cyber defences".

A shocking 19% of affected businesses lost money and valuable data as a direct result of an attack. However, attacks don't have to be successful to be disruptive. Twice as many of the affected businesses (39%) claimed that they'd experienced a negative impact as a result. This included having staff time diverted, needing to put new measures into place or wider business disruption.

Businesses which assume that they have the in-house expertise needed to avoid the most common cybersecurity threats - such as phishing, viruses, hacking and ransomware - may be sadly mistaken.

Hacking, configuration mistakes and disruption to services are three of the biggest risks facing the tech industry. But, there are steps you can take to protect your business's future.

## RISK 1 – HACKING

According to the survey, the sectors most likely to hold personal data about customers include finance and insurance (77%) and health, social work and social care (68%). Information held by these sectors – such as banking credentials and medical records - are sought after on the Dark Web.

For Medtech companies, in particular, the risk of data loss should be the subject of board level discussions. In the last five years, the number of health apps in the major app stores has doubled to over 300,000. With millions of mobile phone and tablet users now collecting and storing their own health data, it's likely that software companies know more about the average user than their doctor does! If this data was to be leaked, it could cause considerable personal embarrassment for users. It's also hard to imagine how the developers could possibly restore their credibility.

Other tech companies are also not immune to the risk of hacking. The risks to Fintech businesses are obvious. Mediatech businesses have also been targeted. Just a few days after raising US$70 million, Canva, a popular Mediatech unicorn, suffered a well-publicised breach.[2] Orchestrated by the infamous GnosticPlayers, a hacker who had already stolen and attempted to sell data relating to over 900 million users, the hack exposed the credentials of a further 139 million. Seven months later, over four million passwords had been decrypted and Canva was still feeling the effects of negative publicity.

## RISK 2 - CONFIGURATION MISTAKES

We all make mistakes, but some mistakes can have devastating consequences.

An administrator for a VPN provider caused untold reputational damage by accidentally leaving an ElasticSearch Server open and accessible.[3] This exposed sensitive data relating to users' logins, banking credentials and even the websites users had visited, believing their activity to be untraceable. Unfortunately, this was not an isolated incident. A recent study found that 93% of cloud deployments had misconfigured storage services and 'the majority also contained at least one network security exposure that had been left open during deployment'.[4] Half of deployments had unprotected credentials stored in container configuration files. These statistics, coupled with risks inherent from unnecessarily permissive IAM (Identity and Access Management) policies and vulnerable routing, make it clear that many cloud-based deployments are in dire need of regular and thorough security reviews.

## RISK 3 - DISRUPTION TO SERVICE

Connectivity is critical for any business, but especially for those in the tech sector.

Digital functionality is what differentiates fintech businesses from traditional banking providers and user expect 24/7 access to their accounts. Outages – however brief – run the risk of negative publicity and customer churn.

With demand for online services continuing to grow, uptime is crucial to referral-based growth.

For the Medtech industry, lack of connectivity could literally mean the difference between life and death. Devices are not only connected to each other, to networks and to the internet within the confines of a hospital, but in the community too. Remote monitoring services, such as those provided to heart patients during lockdown, are critical to identifying potential issues at an early stage. They also provide the opportunity to update firmware on devices, such as pacemakers, which may have inherent vulnerabilities.

## PROACTIVE WAYS TO PROTECT YOUR GROWING BUSINESS

There are a number of ways to protect your IT assets and avoid the financial losses, data losses, reputational damage and disruption that are part and parcel of a successful cybercrime attack:

### 1. Strengthen your frontline defences

Your employees are your biggest weakness, even when you're a tech business!

After a recent high-profile hack, Twitter said that hackers had targeted employees "with access to internal systems and tools". A BBC article claims that "the consensus in the information security community is that Twitter's employees were likely duped by a spear-phishing attack via a phone call. This involves using friendly persuasion and trickery to get victims to hand over crucial information that enables hackers to infiltrate a company's systems".[5]

Now, with your employees' attention at least partially diverted away from their day-to-day jobs, your vulnerabilities are higher than ever. Luckily, there are several steps you can take to minimise risks.

a. Ensure all users – regardless of age or position – complete online cybersecurity training, such as that provided by the National Cyber Security Centre.[6]

b. Warn users about new phishing scams.

c. Circulate news stories about tech companies affected by cybercrime.

d. Regularly remind them to remain alert, especially when receiving unexpected messages by e-mail, instant messaging apps, text and conference call apps.

e. Discourage them from clicking on links in messages or opening attachments without first verifying that they are legitimate and safe.

f. Make sure users with privileged access to your systems - such as developers and tech support staff - take particularly good care of their login credentials.

We also recommend that you ask employees to forward any suspicious e-mails to report@phishing.gov.uk for investigation.

### 2. Strengthen your remote working technology

Make sure that laptops are kept up to date with the latest security patches and anti-malware software. You can also turn up the sensitivity of your web and e-mail filters and ensure that any remote access technologies such as VPN and remote desktop services remain tightly secured. Now is a good time to consider using a third party to perform regular external vulnerability scans to make sure attackers cannot find an easy foothold into your IT infrastructure.

### 3. Safeguard your on-line meetings

Recent press and social media coverage have brought the security of popular on-line meeting apps under scrutiny. In many cases, these risks are not new and are either acceptable or can be mitigated through configuration or secure working practices. You should:

- Make sure that your employees know how to set up meetings with attendance controls, such as meeting passwords or PIN codes, to prevent 'zoom bombers' or frustrate their attempts.
- Remind meeting facilitators to verify the authenticity of all attendees. Give them guidance on how to check attendee lists and explain what they should do if they identify any unauthorised attendees.
- Ask employees to be alert when clicking on links or downloading attachments within these apps. They should apply the same common-sense thinking as they do when handling e-mails.

### 4. Use Cloud Services securely

Microsoft, Google and Amazon are trailblazers in making Cloud service available to everyone.  For example,

# CHALLENGING COMPLACENCY: IS YOUR TECH COMPANY AT RISK?

Microsoft Office 365, admittedly with a bit of support from Covid-19, have transformed how we do our work on a day by day basis and have helped reduce our dependency on physical office space. However, moving to the Cloud is not without risk, with potential for very public security breaches if things do go wrong.

Listen to our latest webinar to find out more about the steps you can take to reduce the cyber security risks associate with Cloud services.

**5. Consider certification for your organisation**

Cyber Essentials Plus and/or ISO 27001, the Information Security Management Standard, won't just protect your business. These certifications can differentiate you from your competition and reassure potential clients and investors.

**6. Manage your third-party cyber security risk**

Many of us outsource IT and other business services to a third party. These organisations are also at risk of security breaches, so you need to make sure they also take cyber security seriously. Identify 'riskier' third parties, particularly those with whom you routinely share sensitive information, that have access to any of your systems that may hold sensitive data or that manages your systems on your behalf.

Make sure that your contracts with these third parties clearly define responsibilities for information and cyber security and insist that these third parties obtain and maintain externally validated security certification, for example Cyber Essentials Plus or ISO27001. Do not be afraid to ask for evidence in the form of certificates or external audit reports.

**7. Keep an eye on industry news**

Cyber security is a fast-moving topic so it's easy to miss out on the latest news. In April alone, a new working group on cybersecurity for Medtech was founded and guidance published on the Principles and Practices for Medical Device Cybersecurity.[7] We recommend following industry news sites and setting up Google alerts.

## IN SUMMARY

Every business is at risk from cybercrime. Criminals are constantly on the lookout for loopholes to exploit, regardless of company size, location or sector. Contrary to popular belief, the tech sector is particularly at risk, as the services tech businesses provide are predominantly hosted and presented on the internet – the Wild Wild West of our digital world.

All businesses, especially tech, need to increase their cyber security resilience to protect their services, data and reputation. Failure to do so could be catastrophic.

## CONTACT US

If you would like further information on how to protect your business, please contact us:

**Maritz Cloete**
Director of Cyber Security, Clearcomm
mcloete@mks.co.uk

Clearcomm is part of Moore Kingston Smith and provides services including data privacy, cyber security, business continuity and information security.

## REFERENCES

[1] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020
[2] https://support.canva.com/contact/customer-support/may-24-security-incident-faqs/
[3] https://www.vpnmentor.com/blog/report-free-vpns-leak/
[4] https://www.accurics.com/news/press-release/accurics-devsecops-report-summer-2020/
[5] https://www.bbc.co.uk/news/business-53617198
[6] https://www.ncsc.gov.uk/training/top-tips-for-staff-web/story_html5.html
[7] http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf