THE IMPACT OF HACKING ON UK BUSINESSES

2022

TABLE OF CONTENTS

mitigate CYBER

EXECUTIVE SUMMARY

Over the past 12 months, the global average cost of a data breach has increased by nearly 10% - the largest single year increase in the last seven years. Due to the changes in working behaviours, businesses have found alternative methods for daily operations, resulting in a heavy reliance on technologies and online services. This has given cyber criminals additional avenues to exploit and compromise your business. It is now more imperative than ever to secure your devices, protect your people, and mitigate any security vulnerabilities.

This report will focus on the impact hacking has on UK organisations, different types of hacking tactics used by cyber criminals, and how penetration testing can alleviate your company's cyber risk.

ABOUT MITIGATE CYBER

Founded by a team of specialists in cyber security, consultancy and information security, we are a trusted cyber security company with a passion for quality service.

Mission

Our mission is to provide dynamic cyber security services and training that extends beyond technology to encompass people, culture, processes and even the physical environment; to make businesses as resilient as possible to prevent or mitigate cyber-attacks.

Vision

Our vision is to be at the forefront of the race to make cyberspace a safer place for organisations through the provision of dynamic services that respond to the risks and threats posed in an ever evolving digital world.

mitigate CYBER

THE THREAT LANDSCAPE

40%

of UK businesses will experience an attack or breach this year.

80%

of cyber breaches will be triggered by staff error.

45%

of employees receive no cyber security training from their employer.

72%

of UK FTSE 350 boards said they were not trained to deal with an incident.

80%

of breaches are the result of internal threats.

4/10

companies suffer at least one cyber-attack per year.

£3.5m

the average cost of a breach in 2021.

mitigate CYBER

TYPES OF HACKS

In our ever-evolving digital world, businesses are becoming increasingly vulnerable to cyber-attacks. There are many methods cyber criminals use to compromise your data and devices, ranging from phishing to viruses, bait and switch attacks. Cyber threats are extensive, and they are not discriminatory when it comes to which organisation is targeted.

PHISHING

A social engineering tactic used by cyber criminals with the aim to gain access to your devices and accounts, or compromise your financial details.

Phishing involves contacting individuals via electronic communications (i.e., email, text, phone call, and social media messages) to deceive the recipient into clicking malicious links or providing sensitive information.

Phishing is one of the most common methods cyber criminals use, with over **3.4 billion fake emails being sent daily**.

Due to the shift in working behaviours, this has led to an increase in email-related cyber crime, with **47% of employees falling for a phishing scam due to working-at-home distractions**. Not only do phishing attempts target individual people, but they are also used to target your company and employees.

According to **IBM Security**'s 'Cost of a Data Breach Report 2021', phishing was one of the most frequent initial attacks, accounting for 17%.

If a phishing attempt was successful in your organisation, this could intercept your company's sensitive data, gather company financial details, and compromise your company network.

The social media company **Snapchat** suffered from a phishing attack in 2017 – this involved a compromised account sending other users links to a fake Snapchat website were the recipient would input their login credentials, resulting in more than **55,000 compromised accounts**.

PHISHING

Phishing communications are designed to provoke a sense of **fear or urgency** in the recipient, causing them to act quickly without questioning its nature. It is important to know the different forms and features of phishing attempts in order to make them easier to identify:

- **Spear Phishing:** Specifically designed communications that include personal information. This is to deceive one particular individual rather than being universal in their target. These could include: your name, place of work, something you have recently done (i.e., a recent holiday), or information of someone you know (i.e., a co-worker).

- **Smishing:** Short for SMS Phishing. This is when a cyber-criminal contacts you specifically via text message, urging you to click malicious links.

- **Whaling:** This is essentially spear phishing, however, is exclusively aimed at wealthy, high-profile individuals. It isn't uncommon for CEOs to fall victim to this, as whaling is estimated to be a $12.5b industry.

Common phishing identifiers include:

- **Questionable email addresses.**
- **Pressuring language.**
- **Spelling mistakes.**
- **Pixelated images and logos.**

Your employees are your company's first line of defence against cyber-attacks, and so it is crucial to ensure they are equipped and educated in handling attack attempts. One of the most effective ways to mitigate your organisation's risk of phishing is through awareness training.

In fact, businesses can see a 70% reduction in socially-engineered cyber threats when regular cyber awareness training is implemented.

mitigate CYBER

VIRUSES

A malicious software that can replicate itself across computers and spread to other systems. These can then be used to steal login credentials, erase data, corrupt files, spam your email contacts, or even completely take over your device. A virus operates by attaching itself to an existing, legitimate program or document in order to execute its code and remains dormant until specific actions are taken. This can then result in affecting the computer and network it is connected to.

A computer virus can infect any device that connects to the internet, and can do so in various manners: via email, social media messages, file downloads, and through visiting malicious websites or apps. In some cases, a computer virus can also be found on portable hardware which, when connected to a device, will transmit the malware.

Common signs your device has been infected with a computer virus include:

Frequent pop-ups, especially when visiting reputable websites/software.

Random changes to your homepage, file names, or ‘missing’ files.

Slow device performance and/or frequent crashing.

Compromised email accounts or spam emails from company accounts.

Irregular financial activity.

Compromised login credentials.

VIRUSES

A famous case of virus distribution in portable hardware occurred in 1989. A cyber criminal distributed 20,000 infected floppy disks to over 90 countries via postal service. Once the floppy disk was inserted into a computer, the virus remained dormant until the 90th start-up. This then proceeded to encrypt the devices' files and demanded a ransom for software release.

Even though this particular incident occurred over 30 years' ago, don't allow that to mislead you into thinking malware is no longer a huge problem for businesses. In fact, cyber crime is on the rise and according to the Global Risk Report, a business is cyber attacked every 11 seconds, an increase from 40 seconds in 2018.

The most effective ways to ensure your devices and data remain secure against computer viruses include:

- **Using trusted and effective anti-virus software**. These are designed to help prevent, detect, and destroy malware.
- **Regularly perform data backups to minimise company downtime in the event of an attack**. If your files do become encrypted via a virus, you will be able to promptly restore these and continue organisation operations.
- **Avoid visiting malicious websites** or **clicking links to any website pop-ups.**
- Be cautious when **opening attachments or clicking links/images embedded into emails.**
- **Perform regular scanning** of your **network and systems** to detect any irregularities.
- **Educate your workforce** – awareness is key!

mitigate CYBER

BAITING/SWITCH ATTACKS

A social engineering tactic used by cyber criminals as a way to lure individuals. This is done by making false promises of a prize/reward, or by creating a sense of urgency and fear. Baiting attacks relies on the individual to provide login credentials or banking information, which is then used to compromise accounts, devices, and finances.

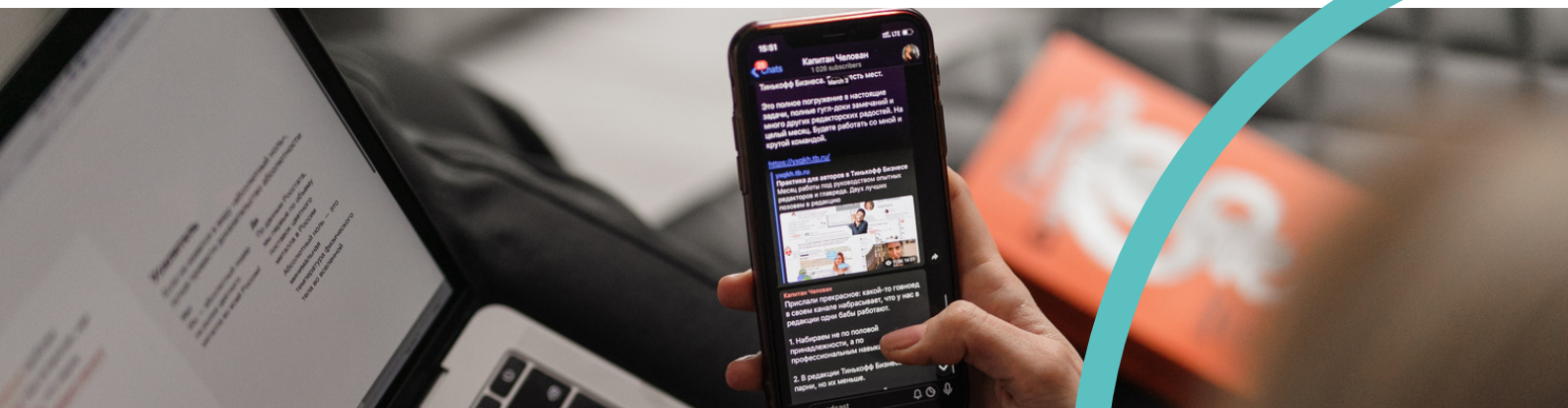
A baiting attack could be done via digital, and physical, means; either by email, website pop-ups, or even by connecting infected portable hardware to a device. Baiting and phishing are both very similar cyber attacks – they are both a social engineering tactic used in the hope recipients click malicious links or provide sensitive information. Therefore, the ways in which to mitigate your risk of a baiting attack is similar to the ways to prevent phishing:

- Ensure you and your employees are aware of the various **social engineering tactics** and are up to date with the **latest attack trends and best practises.**

- Performing **regular phishing simulations** throughout your organisation is a great way to put that knowledge to the test and help you workforce remain vigilant against potential attacks.

- **Be wary of any communications that contain pressuring language**. Key words to look out for include: **“Urgent”, “Request”, “Important”, “Payment”, “Attention”, “Congratulations”**.

- **Trust your gut** – if an offer seems too good to be true, then is usually is.



RANSOMWARE

A type of malicious software that prevents the use of a system, either by locking the system's screen or by locking the user's files unless a ransom is paid. There are various ways a cyber criminal could infiltrate your business, some of the most common being:

- **Embedding malicious links and attachments** in email communications which, when clicked, will start downloading ransomware onto the device.
- **Drive-by-Downloads:** This occurs when a user visits a compromised website which had been embedded with malicious code.
- **Infected Portable Hardware:** Social engineers and cyber criminals will often leave infected hardware in crowded/public places (i.e., an office, café, etc.) hoping a curious individual will connect this to their device which will then deploy ransomware.
- **Open RDP Ports:** Remote Desktop Protocol (RDP) is a huge risk to businesses because many organisations unknowingly have these open. These are designed to allow IT administrators access to an individual's PC for configuration or troubleshooting purposes. Cyber criminals have the ability to access these and deploy ransomware.

Some famous ransomware attacks in recent years include:

2013

250,000 computers running Microsoft Windows were infected in the UK and US.

2015

Targeted gaming data on victims' hard drives in the US and parts of Europe. This demanded a ransom of $500 of bitcoins to decrypt the data.

RANSOMWARE

2017

A world-wide cyber attack that targeted Microsoft Windows computers. This infected an estimate of 300,000 computers, including those in the NHS.

2019 2020

Specifically designed to target large organisations, this ransom was estimated to have accumulated around $150m.

Ransomware attacks are a serious threat to businesses world-wide. Today, ransomware presents a **multi-billion-pound attack vector for cyber criminals** and statistics revealed there were 304 million ransomware attacks in 2020.

All industry types and organisation sizes are in danger of ransomware attacks, to combat the threat and mitigate cyber risk, it is advised businesses implement the following:

- **Create a Continuity Plan:** The plan needs to cover how you would detect the incident, deal with data loss, return to normal operations, and prevent financial penalties.

- **Don't Just Focus on IT:** A ransomware attacks impacts the whole business and not just the IT team, therefore it is important to ensure all departments are aware of the role they play if an attack was to occur in order to be able to respond faster, and deal with the fallout.

- **Improve Security Awareness:** Not only do cyber criminals aim to compromise your devices, but they also look to exploit your people. Those with access to sensitive and confidential data are a prime candidate for cyber criminals, so it is imperative that your workforce know what to look for in potential attack attempts, and are implementing cyber security best practises.

OUR PENETRATION TESTING PROCESS

At **Mitigate Cyber**, our penetration tests identify all known weaknesses in your system. A penetration test can be performed on virtually anything that connects to the internet, including: websites, network infrastructure, mobile apps, IoT devices, and even physical security. Our recommended security improvements protect sensitive internal data, your clients' data, and the infrastructure system which supports it all.

Our penetration test service **Mitihack**, offers a range of services tailored to your organisation:

- **Network Infrastructure:** Our licensed penetration testers will assess your networks security from either an internal or external point of view.
- **Wi-Fi Networks:** Wi-Fi networks are important resources but expose you to common cyber threats to anyone in their proximity.
- **Web Application:** Web application penetration tests identify vulnerabilities which could be accessed through online attacks.
- **Mobile Apps and Devices:** The growth of flexible working means more employees accessing critical data from mobile devices.
- **VoIP:** Our detailed methodology will test for cyber attacks that pose threats to your VoIP systems.
- **Cloud:** Our cloud penetration tests determine how secure your assets in the IaaS, PaaS, and SaaS cloud really are.
- **Database:** Our ethical hackers and qualified consultants will simulate an attack in the same way a hacker would access your database.
- **Social Engineering:** Through digital, verbal, and physical means, our tests will identify weaknesses in your processes and people.

OUR PENETRATION TESTING PROCESS

The typical process you can expect when you take out a **Mitihack** service includes:

STEP ONE

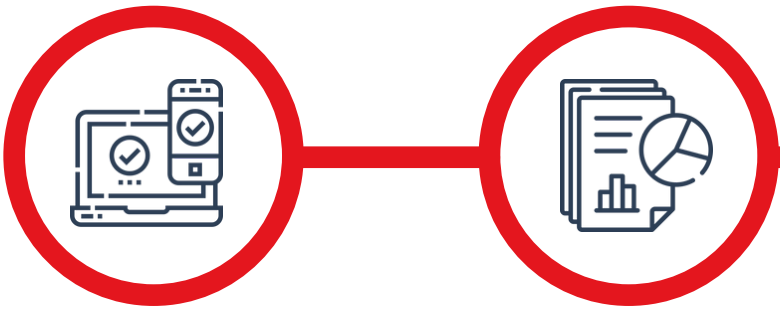
Providing us with information on all systems in-scope that requires testing.

STEP TWO

Our licenced penetration testers will then assess the in-scope items and identify vulnerabilities.

STEP THREE

Controlled attacks are then performed to gain access by exploiting the identified vulnerabilities.



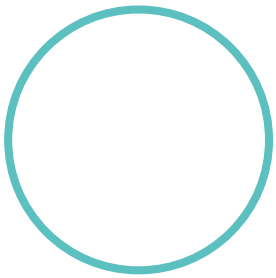
STEP FOUR

Our penetration testers will see whether they can compromise as many privilege accounts and systems while maintaining access.

STEP FIVE

After the test, you will receive a full report along with an in-depth 1:1 meeting to explain the findings and discuss remediations.

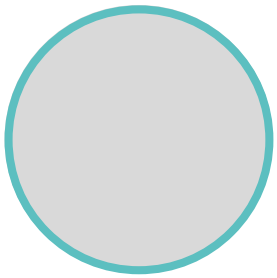
WHITE BOX, GREY BOX AND BLACK BOX PENETRATION TESTING



WHITE BOX PENETRATION TESTING

This involves providing full network and system information to the ethical hacker performing the pen test.

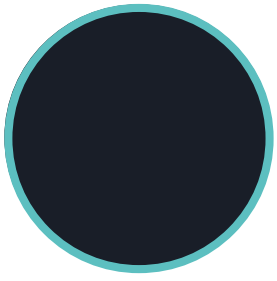
Businesses choose this option as it gives the most thorough evaluation of the business's security.



GREY BOX PENETRATION TESTING

This involves limited network and system information being provided to the ethical hacker (usually login credentials).

This option is chosen as it is a great way to simulate an insider threat, and is an efficient yet effective way to gain insight on the current vulnerabilities.



BLACK BOX PENETRATION TESTING

This involves providing no information at all on the system or network, and is as close to a genuine hack as possible.

mitigate CYBER

WHITE BOX, GREY BOX AND BLACK BOX PENETRATION TESTING

In 2021, our ethical hackers performed 90 penetration tests to various businesses across the UK.

After discussing with our clients the reasons they have decided to perform a penetration test on their systems, one of the most common responses we received was for “peace of mind” following a breach, or a breach of one of their clients. The organisation’s board will then request testing to show the problems and vulnerabilities had been resolved.

Other reasons as to why businesses decide to perform penetration tests include:

- **To meet compliance mandates such as PCI DSS and ISO27001**. It is now also becoming mandatory for particular sectors to carry out periodic penetration tests. For instance, law firms now must perform annual penetration tests in order to be registered with their professional body.

- **For insurance purposes** – some insurance bodies will require businesses to perform regular penetration tests on their systems in order to be covered.

- **When a company is acquiring another company**, they’ll want a penetration test performing as part of the **due diligence process**.

- **When a company implements new technology such as Office 365 or AWS.** As these have a lot of configuration options, and it is common to configure these incorrectly, a penetration test will be able to validate these.

- The **IT team realise there may be some risk in what they’re doing** and want an external perspective to assess their work.

IMPACT ON COMPANIES

Technology is becoming more advanced and sophisticated. These are a huge benefit to our everyday, and working, lives but they can pose serious security risks. Without the appropriate defences in place, this can leave your organisation in an extremely vulnerable position – in fact, **40% of UK businesses are estimated to report a cyber breach this year**. The impact of a cyber breach could include:

- **Company downtime.**
- **Loss of market confidence.**
- **Loss of confidential data and finances.**
- **Reputational damage.**
- **Large fines.**

In 2018, the **Marriott Hotels** experienced a data breach. This involved 300 million guests' personal data being leaked, including card numbers and expiry dates. Even though this breach was reported to the ICO, the hotel group received a fine of over £99 million for failure to comply with GDPR.

Additionally, back in December 2021, a cyber attack had hit more than 300 **Spar** stores. This resulted in many units having to discontinue trading until the incident was resolved. The stores that remained open were only able to accept cash payments due to system downtime.

THE COST OF HACKS

Through today's increasingly connected economy, businesses have come to rely on private infrastructures to host their data, processes, and clients' sensitive information.

As such, businesses have begun to think about their network security seriously, and since there is no excuse for a security breach, your organisation should consider penetration testing as part of the regular security practice.

- **The global cost of a data breach in the UK grew from £2.85m (2020) to £3.14m (2021) – a 9.8% increase.**

- **The cost of a data breach in the UK has increased by 19.7% in the last 12 months. From £2.88m to £3.45m – one of the largest increases worldwide.**

The top **five industry sectors** for average total costs include:

- **Healthcare (£6.83m)**
- **Financial (£4.23m)**
- **Pharmaceuticals (£3.72m)**
- **Technology (£3.61m)**
- **Energy (£3.44m)**

mitigate CYBER

THE COST OF HACKS

Some of the top predicted trends for 2022 include:

- According to the **National Cyber Security Centre** (NCSC), there were three times as many ransomware attacks in the first three months of 2021 than the whole of 2019, and **in 2020 ransomware attacks grew by 485%.** Based on this yearly rise, cyber security professionals are advising businesses be especially vigilant of ransomware attacks over the next few years.

- **Hybrid working is also causing huge vulnerabilities in businesses worldwide** and is expected to do so for quite some time. Certification body IASME has recently reviewed and updated their Cyber Essentials certification process inline with these new working behaviours. Including changes to cloud services, home-working devices, and unsupported software.

- **Third-party risks are also expected to be a significant threat to UK businesses** due to the rise in supply chain attacks from 2020-2021. With major cyber attacks on large organisations over the past 12 months, cyber security professionals are urging businesses to make cyber security a priority in the supply chain of third parties.

mitigate CYBER

PENETRATION TESTING ISSUES BY SECTOR

Even though certain industry sectors are targeted more than others, does not mean that there are those who slip under cyber criminals' radars.

Regardless of company size or sector, if your business processes sensitive data and relies on technologies for daily operations, then you are at risk of a cyber attack or breach.

As a result, many organisation types share cyber security vulnerabilities. According to IBM Security's 'Cost of a Data Breach Report 2021', the most common initial attack vectors over the past 12 months, include:

- **1. Compromised Credentials (20%)**
- **2. Phishing Attacks (17%)**
- **3. Cloud Misconfiguration (15%)**
- **4. Vulnerabilities in Third-Party Software (14%)**

The five top types of records that were compromised over the past 12 months include:

- **1. Client Personally Identifiable Information (44%)**
- **2. Anonymised Client Data (28%)**
- **3. Intellectual Property (27%)**
- **4. Employee Personally Identifiable Information (26%)**
- **5. Other Sensitive Data (12%)**

For additional information on sector vulnerabilities in 2021, see Appendix.

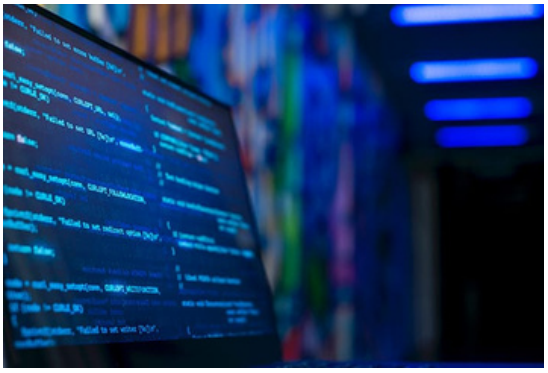
PENETRATION TESTING SERVICES THAT CAN HELP YOUR BUSINESS

NETWORK INTERFACE PENETRATION TESTING

Our licensed penetration tester will test your network security from either internal or external point of view.

WI-FI NETWORK PENETRATION TESTING

Wi-Fi networks expose you to common cyber threats from anyone in their proximity.



WEB APPLICATION PENETRATION TESTING

Web application penetration tests identify vulnerabilities which could be accessed through online attacks.

MOBILE APP & DEVICE PENETRATION TESTING

The growth of flexible working teams means more employees accessing critical data from mobile devices.

mitigate CYBER

PENETRATION TESTING SERVICES THAT CAN HELP YOUR BUSINESS

VOIP PENETRATION TESTING

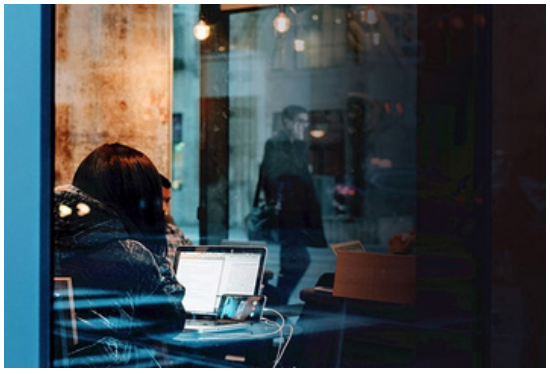
Our detailed methodology will test for cyber attacks that pose threats to your VoIP systems.

CLOUD PENETRATION TESTING

Our cloud penetration tests determine how secure your assets in the laaS, PaaS or SaaS cloud really are.

DATABASE PENETRATION TESTING

Simulate an attack to attempt access into your database.



SOCIAL ENGINEERING

Through digital, verbal and physical means identify weaknesses in your processes and people.

mitigate CYBER

CONCLUSION

Penetration testing is a powerful tool for securing your IT network operations. It provides testers with visibility of security risks and potential vulnerabilities within your network, systems, software, and applications.

One of the best ways to understand how to use penetration testing is by speaking to an experienced cyber security company that knows what they're doing and can advice what your business needs.

This is where Mitigate Cyber comes in. We make use of the best tools and latest technologies, and our ethical hackers are CREST-certified with years of industry experience.

For more information, or to speak to one of our Mitigate Cyber experts, get in contact today!

Are you ready to protect your organisation?

Get in touch

www.mitigatecyber.com/
0333 323 3981
@Mitigate_Cyber
/mitigate-cyber

mitigate CYBER

APPENDIX

Taken from **Verizon**'s '2021 Data Breach Investigations Report'.

Educational Services

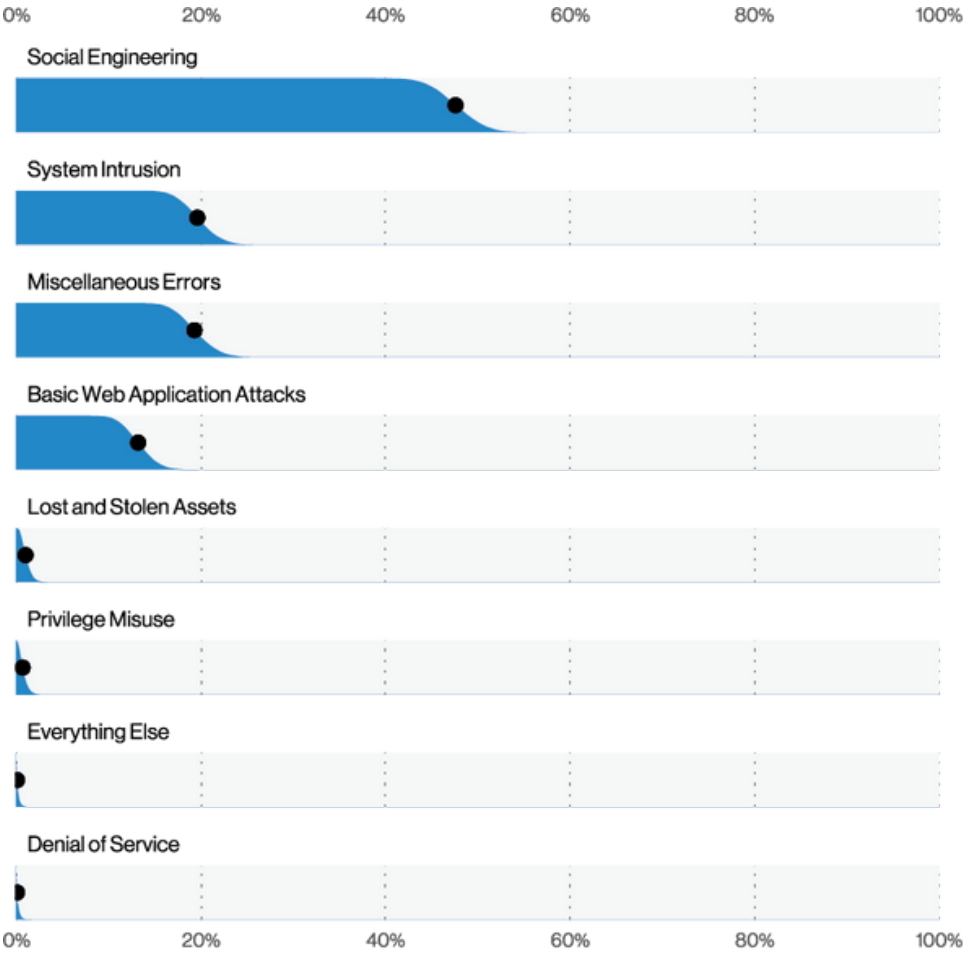


Figure 101. Patterns in Education breaches (n=344)

APPENDIX

Taken from **Verizon**'s '2021 Data Breach Investigations Report'.

Healthcare

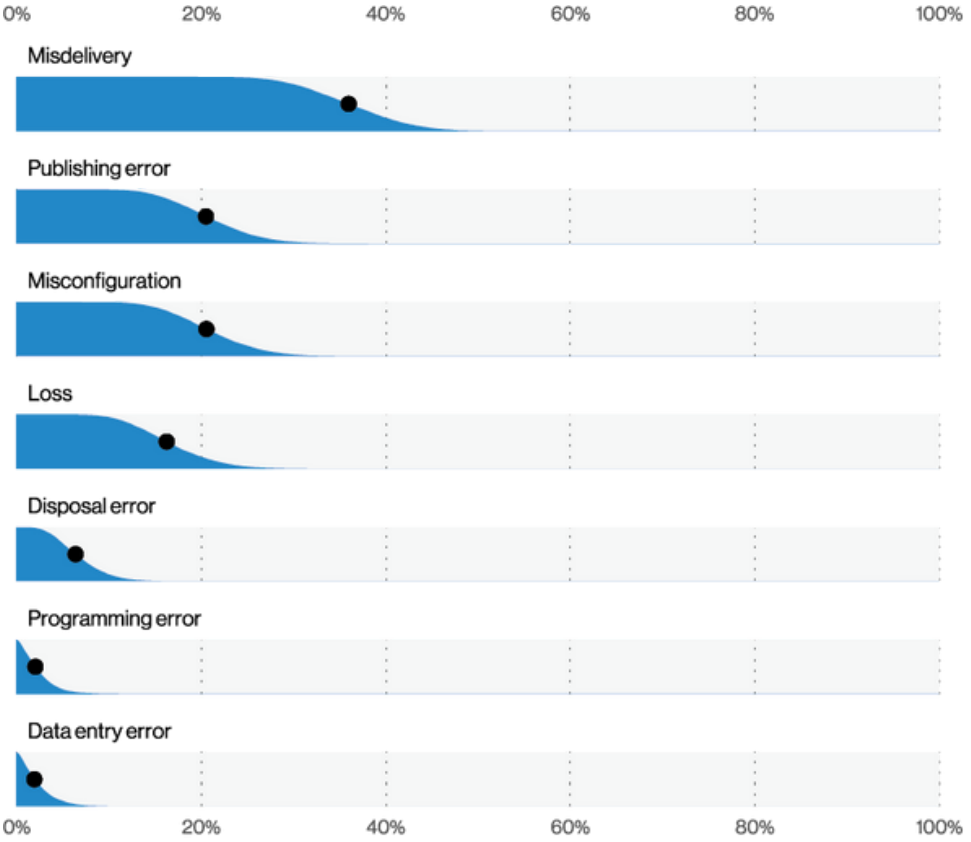


Figure 105. Error varieties in Healthcare breaches (n=70)

APPENDIX

Taken from **Verizon**'s '2021 Data Breach Investigations Report'.

Manufacturing

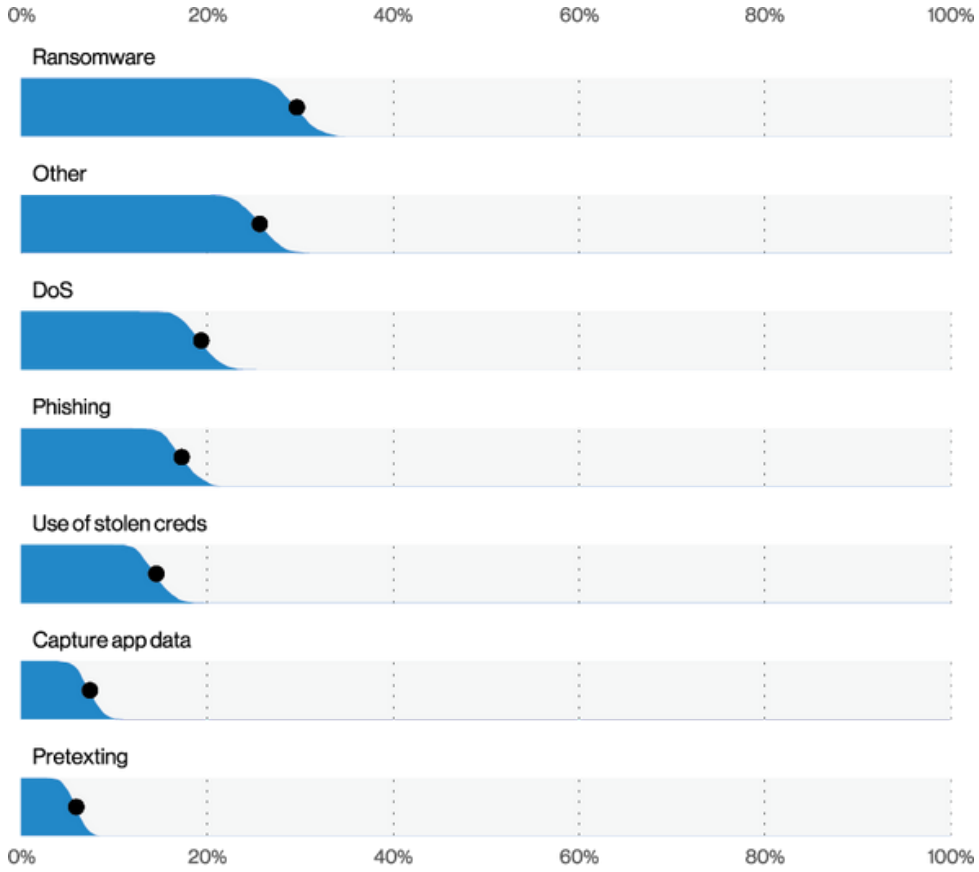


Figure 111. Top Action varieties in Manufacturing incidents (n=476)

APPENDIX

Taken from **Verizon**'s '2021 Data Breach Investigations Report'.

Public Administration

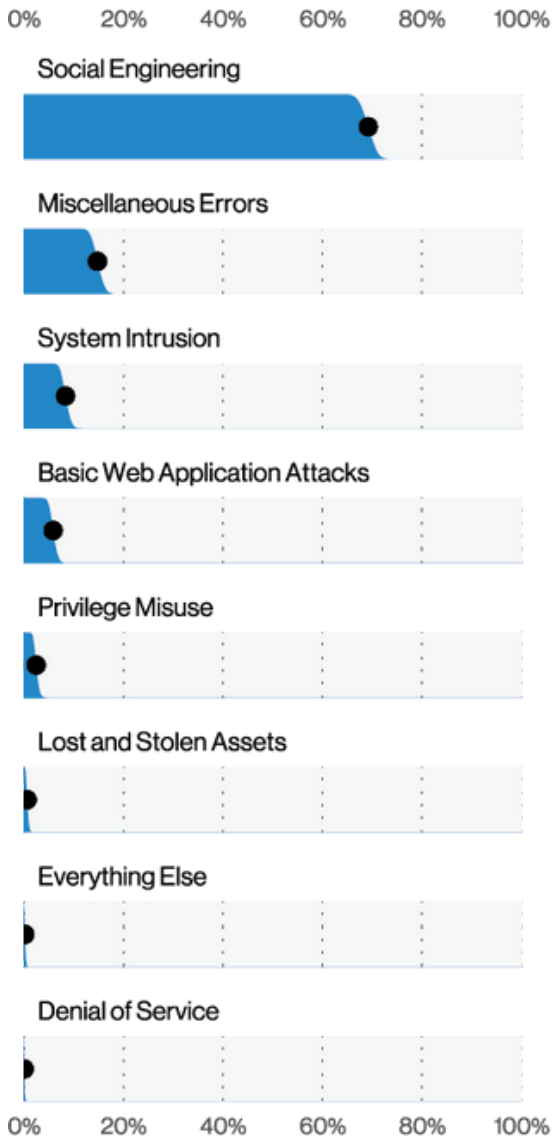


Figure 116. Patterns in Public Administration breaches (n=885)

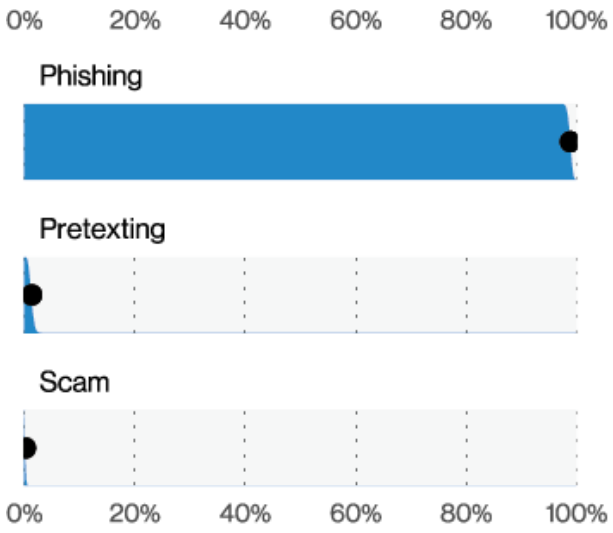


Figure 117. Social varieties in Public Administration breaches (n=611)