Beaming

FIVE YEARS IN CYBER SECURITY

Simple strategies to boost business resilience

Introduction

If you've got a nagging sense that your business should be doing more to protect itself against cybercrime, this guide is for you.

If you think you're already covered, it's for you too, because the threats might not be what you think they are.

New research in this guide shows how cybercrime is a bigger threat than ever. In response, we lay out simple steps about how each size of business can easily protect itself.

Technology and the internet have transformed pretty much every aspect of work and commerce over the last decade or so. Few - if any - can operate as usual should their IT systems be brought down by cybercrime.

And then there is data security. Information has always been power, but now that power comes with greater responsibility. More than ever, businesses are obliged to keep data safe and secure. Failure to do so can be catastrophic.

Beaming goes above and beyond when it comes to providing services that keep businesses, systems and data assets safe. Our network and connectivity services were built from the ground up to be as resilient and secure as possible.

For the last five years we have been running a big research project to understand the evolving threat landscape. We are now sharing that understanding, and using it to offer a simple guide to help businesses of all sizes keep safe. We believe it is the first of its kind to explore cyber security trends over such an extended period.

We hope our insight and guidance help businesses of all sizes understand the risks and take steps to reduce them.

Sonia Blizzard, Beaming

Beaming

Contents

Note: in the report, the following terms are used to describe businesses

Solo	1 person
Micro	2-10
Small	11-50
Medium	51-250
Large	251+

The Big Picture

Take a look at how cybercrime and cyber security have changed over five years based on Beaming's 2015-2019 cybercrime study.

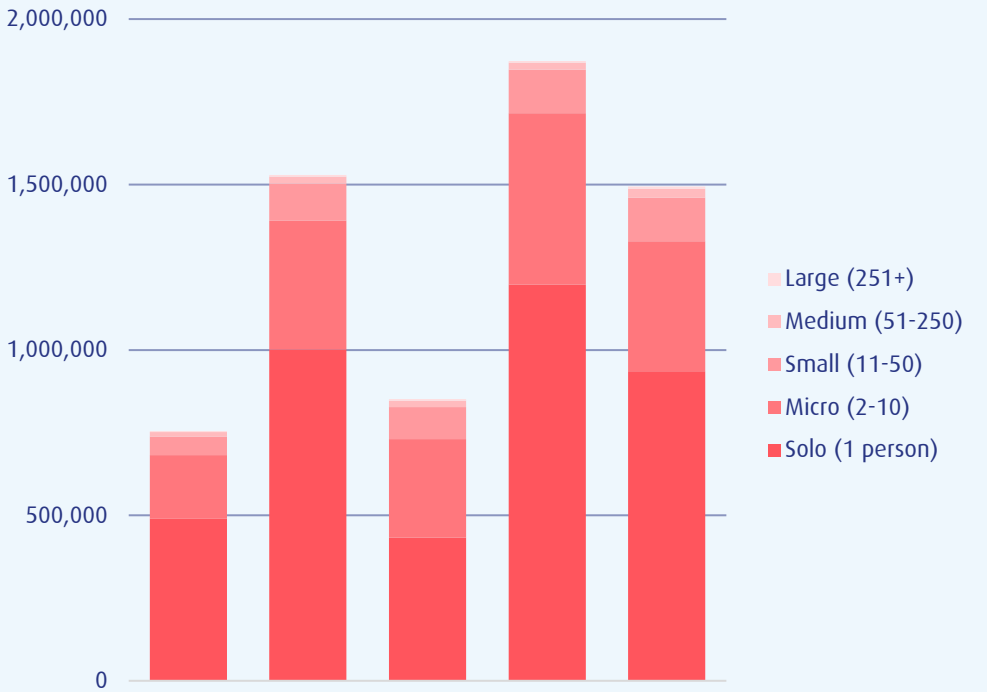
The cybercrime rate has doubled in the last five years

The number of UK businesses succumbing to cyber-attacks has doubled in the last five years, with the most significant growth in victim rates coming in the small-business community.

In 2019 a quarter (25%) of all UK businesses fell victim to cybercriminals. This equates to 1.5 million companies. That is up from 755,000 (13%) in 2015.

Phishing and malware were the attacks most likely to breach businesses in 2019. 9% of companies fell victim. These have been constant threats over the last five years.

Estimated number of cybercrime victims by business size 2019

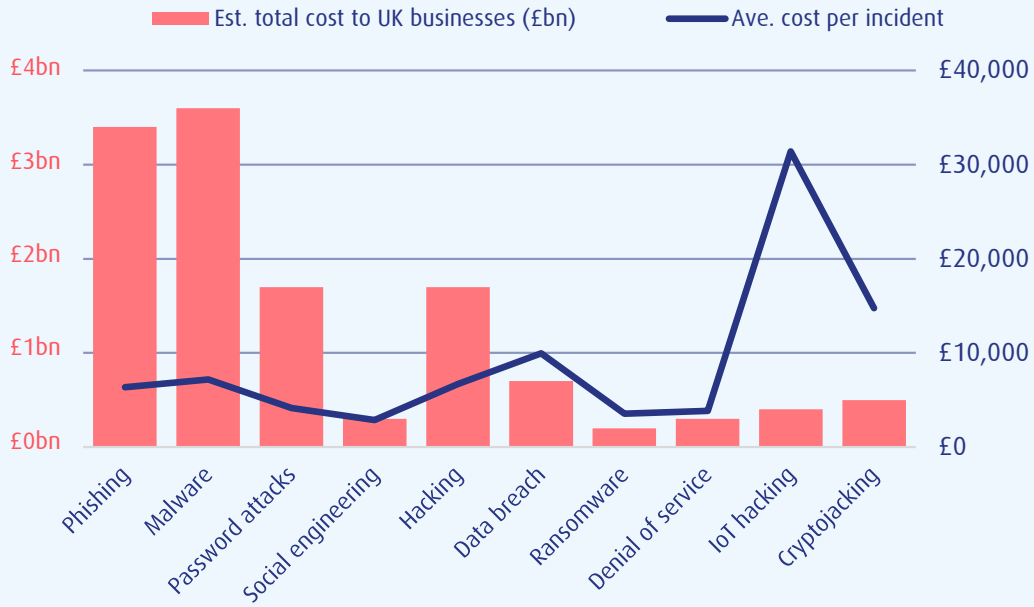


Source: Beaming and Opinium, January 2020

The costs to business are huge

- Beaming calculates that UK businesses lost almost £13 billion due to cybercriminals in 2019.
- The total cost of cyber security breaches over the last five years - including damaged assets, financial penalties, and lost productivity - is probably more than £87 billion.
- The average cost of breaches has fallen, from £26,000 per incident in 2015 to £6,000 last year, reflecting their now indiscriminate nature and the vastly increased volume of breaches at small businesses.

The business cost of cybercrime incidents in 2019



Source: Beaming and Opinium, January 2020

Businesses are getting more concerned...

- What used to be considered a big-business and IT managers' problem has become a severe concern affecting all employees in all sizes of business.
- More than a fifth of small (20%), medium (24%) and large companies (36%) now discuss a range of cyber threats at board level, while the proportion of businesses taking additional steps to mitigate a variety of cyber-risks has increased from 16% in 2015 to 37% last year.
- Malware continues to be the biggest concern for business leaders, with 45% now taking additional measures to combat it (compared to 26% in 2015).
- Hacking and password attacks, where criminals try to access systems using scripts that run a wide range of possible password combinations, were also among leaders' prominent areas of concern.

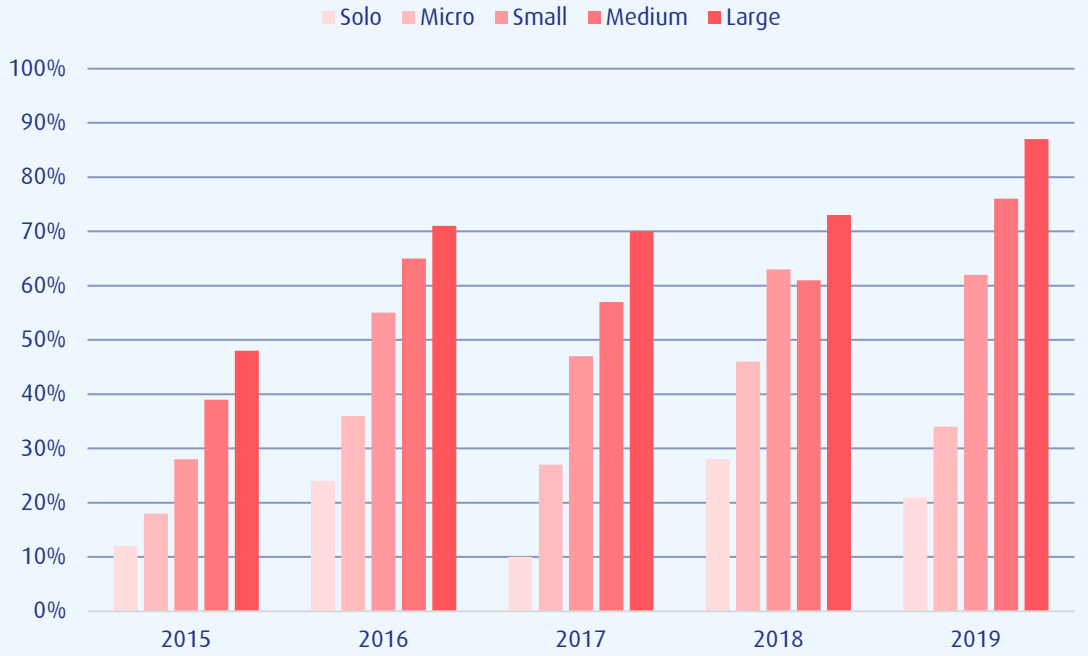
... but that does not always translate into action

- Only 9% of businesses have a documented cyber security policy.
- Only 10% carry insurance against cybercrime.
- Only 10% have an intrusion-detection system.

Size matters when it comes to cyber security

- More people means more sources of vulnerability. The risk of falling victim to cybercrime increases by more than 60% when a business hires its first employees.
- Staff members were identified as being responsible - either through malicious intent, neglect or genuine mistakes for breaches in more than a third of cases.
- Business leaders said employees contributed to 37% of breaches in 2015, and 36% in 2019.

The proportion of businesses reporting falling victim to cybercrime 2015 - 2019



Source: Beaming and Opinium, January 2020

Small businesses are now on the front line too

- As companies grow, they are more likely to fall victim to cybercriminals. Larger companies were breached consistently at a higher rate than smaller businesses over the last five years.
- Companies employing more than 250 people were breached at the highest rate throughout Beaming's study, culminating in nine out of every ten large organisations (87%) falling victim in 2019.
- Small businesses, however, experienced the steepest rise in victim rates, increasing from 28% of 11-50 person firms in 2015 to 62% last year.
- Small businesses are now on the front line in the war against cybercrime. But they haven't invested in cyber security or employee education at the same rate as their larger counterparts, and are an easier target as a result.

Getting Cyber Secure

Simple strategies to boost business resilience in 2020

Cyber security can be confusing.

That's why we have developed a new self-evaluation tool – Beaming's Hierarchy of Cyber Security Needs – which allows business leaders to assess how well they are doing with cyber security and data-protection, as well as the simple steps and strategies they should probably take next to boost business resilience.

While the number of attacks and breaches - and the level of board-room concern - have never been higher, uptake of more sophisticated cyber security measures remains relatively low. For example, just 8% of micro-businesses and 15% of small ones have documented cyber security policies in place today.

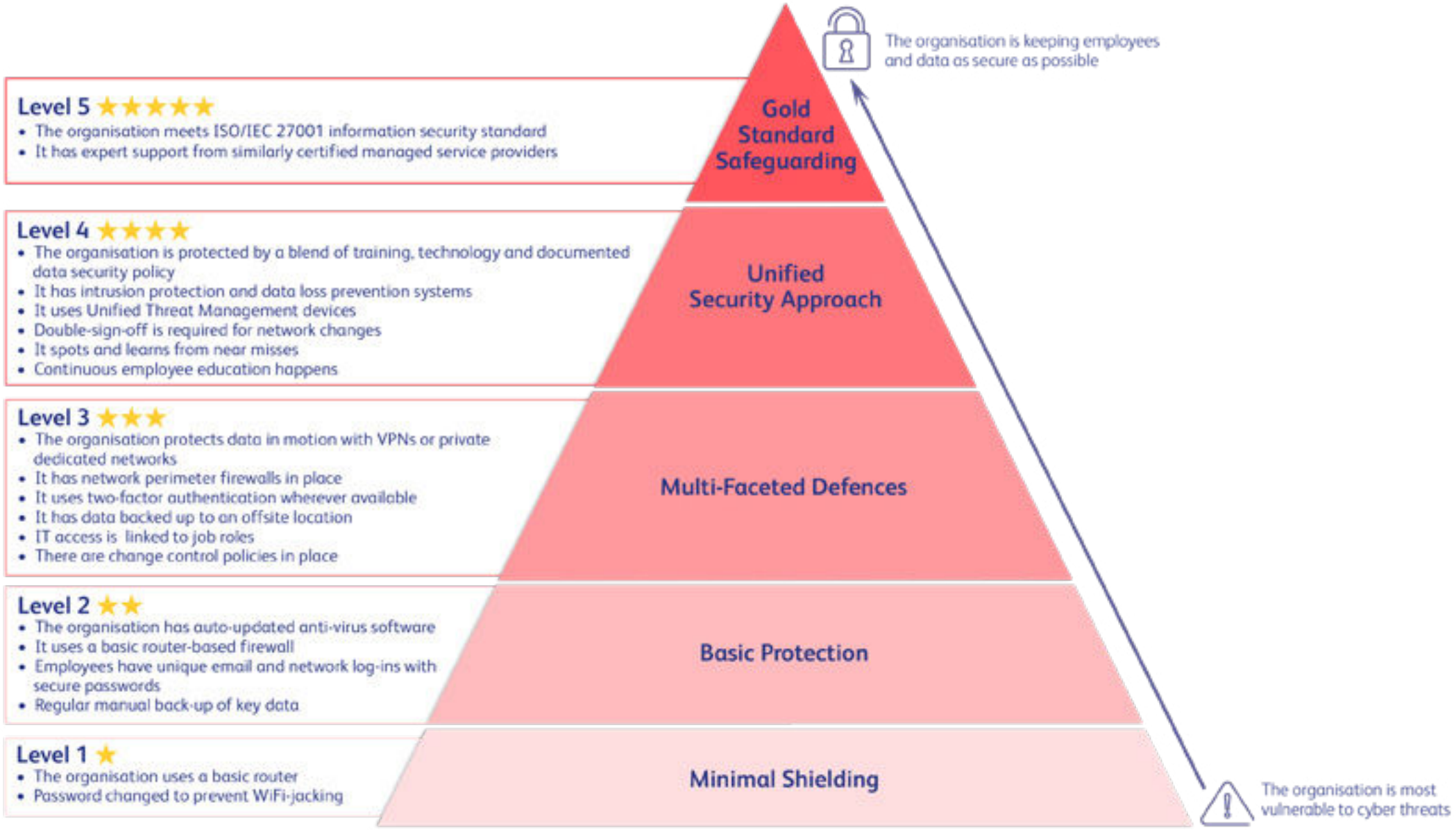
The vast majority of companies are effectively making cyber security up as they go along. We need to change that.

Part of the problem, especially for smaller businesses wanting to improve their resilience to cyber-attacks, is to understand what good cyber security looks like. This is where the Hierarchy of Cyber Security Needs comes in.

We have created the following graphic so businesses can easily look at what level of protection they currently have from the measures implemented, and what they need to do to increase protection.

Beaming's Hierarchy of Cyber Security Needs

How does your business perform and what steps do you need to take to move to the next level?



How do differing levels of protection affect vicitim rates?

We placed the respondents to our January 2020 survey in to each of Beaming's Hierarchy of Cyber Security Needs levels and compared how each level has been affected by various cyber threats.

Estimated proportion of UK businesses at each level on Beaming's Hierarchy of Cyber Security Needs

	Least protected businesses → Most protected businesses				
	Level 1	Level 2	Level 3	Level 4	Level 5
All	61%	11%	1%	< 1%	< 1%
Solo	59%	9%	1%	0%	0%
Micro	69%	20%	2%	1%	0%
Small	58%	19%	1%	1%	0%
Medium	40%	10%	1%	1%	1%
Large	43%	15%	5%	2%	1%

Source: Beaming and Opinium, January 2020

Cybercrime victim rates by Beaming's Hierarchy of Cyber Security Needs level in 2019

	Least protected businesses → Most protected businesses				
	Level 1	Level 2	Level 3	Level 4	Level 5
Hacking	7%	10%	0%	0%	0%
Data Breach	6%	7%	0%	0%	0%
Cryptojacking	3%	6%	10%	0%	0%
IoT hacking	3%	4%	0%	0%	0%
Social Engineering	8%	14%	0%	0%	0%
Password attacks	12%	13%	0%	0%	0%
Phishing	28%	31%	0%	0%	0%
Denial of Service	5%	7%	0%	0%	0%
Malware	18%	29%	0%	0%	0%
Ransomware	4%	8%	0%	0%	0%
NET: VICTIM	48%	64%	10%	0%	0%

Source: Beaming and Opinium, January 2020

Key Threats to Businesses Today

Threat 1: A flood of indiscriminate cyber attacks

UK businesses are under siege from cyber-attackers, and their virtual castle walls are often not strong enough to hold firm. In 2019, twice as many businesses fell victim to cyber-attacks as in 2015.

The number of cyber-attacks doubled between 2018 and 2019

- In the time it takes you to read the next five sentences, every business in the UK with an internet connection will, on average, have been attacked online at least once.
- 2019 was the worst year on record for the volume and variety of cyber-attacks on UK businesses.
- The average UK business was attacked online 576,000 times, more than once a minute. That was double the number of attacks the year before (281,000).
- The vast majority of these attacks were thwarted.
- But the increased use of Bots to automate attacks and find the most vulnerable businesses means any crack in cyber security is more likely to be found than ever before.

Victim volumes doubled between 2015 and 2019

- In 2019, 25% of UK businesses fell victim to successful cyber-attack - almost twice as many as in 2015 (13%). Businesses are twice as vulnerable today as they were five years ago.
- In each of the past two years, 1.5 million or more businesses have been compromised, up from 755,000 in 2015.
- Among UK businesses with at least two members of staff, a massive 40% were victims of a successful cyber-attack - twice as many as in 2015 (19%).

Cybercrime victim rates by threat in 2019

	All	Solo	Micro	Small	Medium	Large
Phishing	9%	6%	17%	29%	29%	38%
Malware	9%	7%	12%	20%	21%	31%
Password attacks	7%	6%	9%	11%	18%	23%
Social engineering	2%	1%	4%	11%	17%	25%
Hacking	4%	4%	4%	8%	11%	22%
Data breach	1%	0%	3%	11%	19%	18%
Ransomware	1%	0%	4%	5%	13%	23%
Denial of service	1%	0%	6%	0%	18%	16%
IoT hacking	0%	0%	0%	3%	16%	20%
Cryptojacking	1%	0%	2%	4%	10%	16%

Source: Beaming and Opinium, January 2020

Threat 2: Small businesses are now much more vulnerable

Small businesses are leaving their doors unlocked, and criminals are taking advantage. The most significant increase in victim rates since 2015 has been among small businesses.

Nearly two-thirds of small businesses now fall victim every year

- The number of victims in this sector is growing faster than that in any other. 28% of the population fell victim in 2015; 62% did last year.
- In part, this is because smaller businesses are easier targets.
- In January 2020, 69% of micro-businesses and 58% of small companies had only minimal levels of cyber security protection in place. They relied on anti-virus software and basic router protection only.

Some small businesses are not keeping pace with changes in cybercrime

- Small businesses can easily misunderstand the nature of cybercrime. Mainly it is automated attacks, driven by algorithms and Bots, that scour the internet looking for any vulnerabilities.
- You might think you won't be a target because you are too small to interest the hackers or cybercrime syndicates. But most attacks are indiscriminate.
- If a Bot can infiltrate or steal from a small charity more easily than a giant corporation, it will take down the charity first.
- Many business leaders, particularly at the smaller end of the spectrum, don't recognise the threat. Or they wrongly assume that their broadband router and antivirus systems will be sufficient. Most need to do more to protect themselves.

By climbing Beaming's Hierarchy of Cyber Security Needs from level 2 to level 3, you'll improve your resilience to phishing attacks. In 2019 31% of businesses sitting at level 2 fell victim to phishing, but no businesses at level 3 succumbed to this type of attack.

Threat 3: The rise and rise of Phishing – and how to stay safe

Almost half the successful attacks on businesses with employees in 2019 used phoney emails. Phishing is now the most successful form of cyber-attack.

Phishing is growing, and businesses are biting

- In 2015, businesses were most likely to fall victim to malware - downloaded programmes or files harmful to IT systems.
- Malware remains a significant threat, but a near tripling of victim rates from Phishing expeditions over the last four years means that any company with employees is now most vulnerable to this form of attack.
- Phishing attacks try to get sensitive information such as usernames, passwords and credit card details by posing as a trustworthy entity such as the company's bank. It happens mainly in email but increasingly through spoofed phone calls.
- Phishers often direct users to enter personal information at a fake website, which mirrors the look and feel of the legitimate site.

Top cyber security threats by business size 2015- 2019

	2015	2016	2017	2018	2019
Solo	Phishing 6% Malware 5% Denial service 4%	Phishing 18% Malware 7% Denial service 4%	Denial service 5% Phishing 3% Malware 2%	Phishing 23% Malware 8% Ransomware 2%	Malware 7% Phishing 6% Password att. 6%
Micro	Malware 8% Phishing 6% Denial service 4%	Phishing 26% Malware 16% Denial service 8%	Phishing 22% Malware 14% Social eng. 10%	Phishing 26% Malware 17% Password att. 14%	Phishing 17% Malware 12% Password att. 9%
Small	Malware 14% Phishing 11% Hacking 4%	Phishing 26% Malware 22% Data breach 18%	Phishing 22% Malware 14% Hacking 11%	Phishing 26% Malware 17% Password att. 14%	Phishing 29% Malware 20% Data breach 11%
Medium	Malware 17% Denial service 12% Phishing 11%	Malware 27% Phishing 22% Hacking 16%	Malware 20% Password att. 17% Phishing 13%	Malware 34% Phishing 29% Hacking 21%	Phishing 29% Malware 21% Data breach 19%
Large	Malware 21% Hacking 16% Phishing 15%	Malware 37% Phishing 28% Data breach 24%	Phishing 27% Social eng. 19% Malware 18%	Malware 34% Phishing 29% Hacking 21%	Phishing 38% Malware 31% Social eng. 25%

Source: Beaming and Opinium, January 2020

10 Simple Steps for Increased Resilience

We recommend that all small and medium sized enterprises achieve at least level 3 and start work towards becoming level 4 on Beaming's Hierarchy of Cyber Security Needs (page 8). The most immediate measures to put in place are as follows:

1. Ensure anti-virus software is installed and updated automatically on every device used to access company systems.

2. Secure your internet router. Speak to your ISP to ensure you're using the latest hardware. Enable automatic updates. Change default usernames and passwords. Deactivate WPS

3. Ban password sharing. Every employee should have a unique username and password to access company systems. Use secure password management software and super-secure passwords to access it.

4. Backup your data, preferably in multiple copies. The risk of ransomware makes it most important to backup company data. Use your own servers in specialist co-location facilities for your most sensitive information.

5. Introduce two-factor authentication. Reduce your exposure to password attacks by requiring multiple credentials, such as a secure password, approved device and physical token, to access systems.

6. Adopt a 'least privilege' policy. Limit individual user's privileges so that they can only access the files, data and systems they need to do their jobs.

7. Invest in VPNs or private dedicated networks. These use dedicated connections and specialist protocols to secure data between sites. They are vital with increased use of cloud computing and remote working.

8. Put in place a network-perimeter firewall. This provides an extra layer of protection for your company by filtering traffic entering and leaving your network across multiple locations and internet connections.

9. Educate employees, particularly around the threat posed by phishing. Have a look at our Business Guide to Phishing and make sure all of your employees are familiar with its advice.

10. Engage a specialist IT professional or cyber security expert to support you. This could include a trustworthy managed service provider like Beaming.

Cyber Security Jargon Buster

The key terms business leaders must be aware of to boost business resilience

Anti-virus software: Also known as anti-malware, this is a computer programme used to prevent, detect, and remove malware. Keep up to date: Cyber-crime evolves fast. Heed the advice and install updates from your software and IT platform providers.

Bots: Bots are used on the internet to automate simple, repetitive tasks at high speed. When programmed maliciously, they can be used to carry out denial of service attacks or log keystrokes and gather passwords.

Clearing up after leavers: Don't leave old email accounts and access routes to the network dormant. Delete them to eliminate a potential source of vulnerability.

Cyber insurance: An insurance policy that covers financial losses if you're the victim of a cyber-attack or data breach.

Cyber security policy: A documented set of procedures stating what your business will do to protect itself and employee responsibilities. Make sure you have appropriate policies and procedures for data security and access control. Make sure they are regularly updated and communicated to all members of staff, including the Board.

Data back-up: Making copies of business data that can be accessed if the original source is corrupted or stolen. While this can be done manually using storage devices, or automatically to a public cloud provider such as Google or Amazon, it is safest to mirror your systems and data to your own dedicated servers located in a data centre or a colocation facility.

Data breach: When people who should not see secure or sensitive information gain access to it. The data might be financial, confidential or contain trade secrets.

Denial-of-service attack: An attack that stops businesses using a vital IT resource, or which prevents customers from connecting with you.

Employee education: A policy is useless if it doesn't become part of your practice. Provide a simple guide and set of procedures for staff, and train them in simple cyber security.

Intrusion detection/prevention system: A device or software that detects anomalies to catch hackers before they do real damage to your network.

ISO/IEC 27001: Top level information security standard requiring organisations to adopt overarching management processes to ensure controls continue to meet the security needs on an on-going basis. Organisations must examine cyber risks systematically, and implement comprehensive controls to address risks deemed unacceptable.

Least-privilege policy: This means making sure each employee has the lowest level of user rights required to do his or her job. This minimises the number of potential sources of vulnerability and the impact of successful attacks.

Malware: Software designed to infiltrate and then disrupt or damage a computer system. Viruses, worms, spyware and Trojans are all malware. Almost always disguised as something innocent-looking.

Manual back-up: Backing up is making a copy of your data somewhere you can get to it if your original data is corrupted or stolen. Manual back-up means someone has to take on the job of backing up and make the copies themselves.

Multiple eyes on the prize: Don't rely on one person for firewall configuration, software updates and access control. If you have only one IT person, use another company's support. Make sure significant IT changes have two experts checking them for security before completion. Work with ISO27001 certified suppliers wherever possible.

Network-perimeter firewall: The first line of defence against external attacks, unwanted traffic and dangerous content. This is a secure boundary limiting network access to trusted data and sources only, and stopping outgoing traffic from accessing potentially harmful networks and hosts.

Phishing: Attackers send fraudulent emails that look like they are from a reputable company to dupe victims into granting access to malware or divulging sensitive information such as usernames, passwords and credit-card details.

Proactive vulnerability scanning: Software used to identify weaknesses in a computer network. This allows network security to be improved ahead of any potential cyber-attacks.

Ransomware: Malware that blocks access to data on your computer or network, often by encrypting access to it, and demands payment for access.

Record near-misses: Have processes in place for documenting and analysing near-misses for data breaches and use this as the basis continuous improvement.

Router-based firewall: A firewall built into the router you use to connect to the internet, providing a barrier between your internal systems and untrusted external networks.

Trojans: Just like the mythical Trojan Horse, Trojans mislead IT users about their intentions. They are programmes that look innocent but are dangerous. Ransomware attacks often rely on Trojans to infect a victim's computer.

Two-factor authentication: Two-factor or multi-factor authentication is the practice of asking a user for two or more pieces of identity information. An employee might, for example, have to use a password and an approved device, to gain access to a system.

Unified threat management: A cyber security tactic which employs a single hardware or software installation to do several security jobs. This holistic approach simplifies installation, configuration and maintenance.

Unique email and network log-ins: Don't share log-ins. Make sure all your passwords are strong, only used by one user, and that employees are not using their company passwords anywhere else.

Virtual Private Networks: A Virtual Private Network or VPN is a secure connection linking users in different locations. The VPN encrypts the data, meaning anyone who intercepts it will not be able to read it.

Web-application firewall: Many businesses now depend heavily on web-based applications such as Microsoft 365. A Web Application Firewall helps protect web applications from attack and corruption by monitoring traffic between a web application and the Internet.

About Beaming - www.beaming.co.uk

If you want support with keeping your company safe, call Beaming. We are a specialist Internet Service Provider (ISP) for businesses and unlike most providers, we own our network that has been built it for top-quality business performance. We supply thousands of organisations across the UK with fast, reliable, and secure voice and data connectivity and managed services.

Cyber security is at the forefront of everything we do, and we are ISO27001 certified - the gold standard in data safeguarding. We can help you increase your resilience cyber-attacks.

Our teams are handpicked, not only for their great technical capabilities but their great people skills too. Our customers never end up talking to robotic sounding call centre operations. Whether advising you on the best package or helping you choose an upgrade for your growing business, we do it in a way that is honest, human, friendly and fast.

Follow Beaming online and on Twitter to get regular updates on cyber threat analysis and new cyber security insights.

Beaming

How to get in touch

Speak to our experts:
Call 0800 082 2868
Or email hello@beaming.co.uk
Or visit www.beaming.co.uk

Certificate Number 9849
ISO 9001, ISO 27001