BULLETPROOF

BULLETPROOF ANNUAL CYBER SECURITY INDUSTRY REPORT

2020

www.bulletproof.co.uk

CONTENTS

FOREWORD FROM OUR CO-FOUNDER

Finding the right approach to cyber security

Too many organisations are operating blind and **failing to see the threats**, let alone prevent them.

I'm pleased to introduce our second annual cyber security review. We've gathered an insightful set of global data from our own research, intelligence and honeypots to provide a thought-provoking look into the world of cyber security.

What's clear from all this data is that, although every year we hope for a dramatic improvement in corporate security, we continue to see a lot of the same mistakes being made over and over again. The breaches we see reported in the news can often be attributed to businesses failing to meet best practices.

In our 2020 report, we address the interesting trends shown by our data and discuss the innovations being made by a constantly evolving hacking community. It often seems as though organisations are outmanned and underprepared when it comes to cyber security. This means, that whilst hackers are making their own advances, they're often simply exploiting the same old flaws or misconfigurations they always have.

We have high expectations of our staff and we continue to build up our threat data, investigate events and produce innovative technology in order to keep our customers secure.

In this report, we analyse real data from a number of areas including:

- Our penetration tests.
  Including but not limited to:
  - Application penetration tests
  - Phishing
  - Internal and external infrastructure
- Our SOC data
- Forensics
- Scanning data

Through this we have been able to provide a unique perspective to businesses, helping them to see the real threat landscape and not just the over-hyped attacks.

This report covers many verticals and ensures that all insights are valid and useful to all organisations. It has been written in a way that reduces fear, uncertainty and doubt, and it caters not only to deeply technical people, but also someone who requires the facts to support business decisions.

Getting the basics right is critical and yet businesses continue to fail to implement security by design, leading to an increased attack surface and unnecessary risks. The importance of threat detection is a priority and is still the best way to keep ahead of the hackers. Too many organisations are operating blind and failing to see the threats, let alone prevent them.

I hope this report provides valuable food for thought and helps you find the right approach to cyber security, whether you are a decision maker looking to source a new solution, or a developer building the latest applications.

Oliver Pinson-Roxburgh
Co-founder

EXECUTIVE SUMMARY

Best practice is the key to security

If we were to summarise this report in two words, they would be 'best practices.' That is to say they are not being followed. Security and privacy by design are not being incorporated, leading to a huge amount of unnecessary risk.

Our penetration testing results show that the most pervasive of critical flaws, offering hackers an easy opening into an environment, are once again outdated components. Unpatched or unsupported software was the biggest threat in 2018 and continues to be now.

1 in 5 Bulletproof tests revealed a critical flaw, with as much as 34% of tests featuring a high risk. Despite businesses being increasingly driven by regulations and their customers to improve security, these figures show that it's not an easy task. Securing data is difficult and there are traps lurking everywhere and the average attack surface is growing. Customers are interacting with businesses in a variety of different ways from mobile applications and IoT devices to websites and more. Keeping all these avenues secure, whilst maintaining usability and agility is a challenge. This challenge is compounded by a shortage of cyber security experts, so it's not surprising that we're still seeing critical issues.

Securing data is difficult and there are **traps lurking everywhere**.

This report highlights several key industry stats taken from our penetration test results, SOC data and compliance consultancy reports, which paint the clear picture that best practices are not being followed. Some of the most intriguing findings are:

- **1 in 5** penetration tests revealed a critical risk in need of immediate remediation
- The number of **medium risks** outnumber the **low-risk issues**
- Over **half of security events** relate to user activity
- Services are discovered and attacked within **32 milliseconds** of going live
- **50%** of **critical flaws** refer to **outdated** or **unsupported components**
- Cloud services **are not** innately secure
- AI voice technology was used in **successful CEO fraud**, confirming a prediction we made last year
- **68% of malicious IPs** encountered this year were known **bad actors**
- **Privacy** and **security** by design is not being followed

Our data highlights the overall state of security and offers a good representation of the challenges organisations will be facing in the near future. Too many businesses are failing to spot the indicators of compromise until it's too late. Spotting them without the right tools and knowledge is difficult however. This report provides a balanced view from the perspective of both red teams (hacker's perspective) and blue teams (defender's perspective).

Understanding both areas is necessary to forge a strong security strategy and stop hackers in their tracks. This Bulletproof report will help you decide what you need to do to keep your business secure in an evolving threat landscape.

OUR REPORT FINDINGS AT A GLANCE

Key data and recommendations

Better Patch Management

1 in 5 tests **revealed a critical flaw**.

The **Education sector** contained the **highest number of critical flaws**.

New compliance mandate pushes for **privacy by design**.

Improve Intelligence

Cyber attacks against UK business **up 243%** in Q3 2019.

68% of malicious IP addresses targeting our honeypot known for **SSH brute forcing**.

Insider threats are a prevailing concern for businesses.

Improve Detection and Response

Services are **targeted by hackers** within **32ms of going live**.

Over **4,000 malicious login attempts** against Office 365 in **one month**.

Ransomware attacks up 77% in the first half of 2019.

Accidents and **human error** are a key risk to business security.

Employee Education and Training

3.4 billion phishing emails are sent daily.

50% of critical flaws across all tests were due to **outdated components**.

74% of businesses feel they **don't have the staff** to protect themselves from cyber threats.

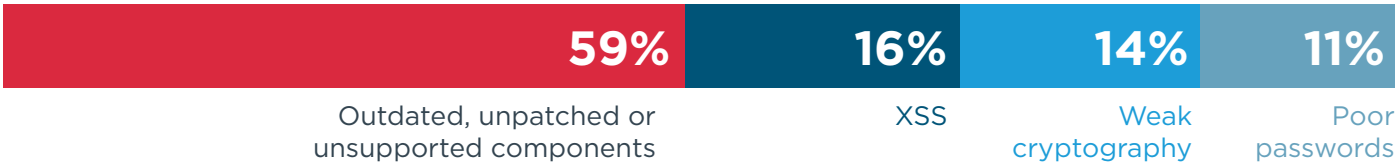
OUR REPORT FINDINGS IN NUMBERS

MOST COMMON CRITICAL FLAWS

Hackers are always looking for weaknesses to exploit. Critical flaws offer an open door for them to get in. These are the most common critical flaws discovered in Bulletproof's penetration tests:

TOP RISKS 2019

TOP RISKS 2018



Budget allocated to cyber security in healthcare is **1-2%** compared to the average **4-10%** of other sectors.[20]

TOP HIT INDUSTRIES ACCORDING TO OUR STATS

Outdated software
Education, Construction and Automotive

Weak encryption
IT, Healthcare, Marketing, Entertainment and Leisure and Insurance

Sensitive information disclosure
IT

Attacks against SMEs increased by **243%** in 2019.

20 https://www.thelancet.com/pdfs/journals/landig/PIIS2589-7500(19)30005-6.pdf

COMMON WAYS HACKERS MAKE THEIR MONEY

The largest proportion of attacks we see are organised criminal gang related, where attacks are run like businesses with the focus on making money. These are some common ways hackers monetise attacks:

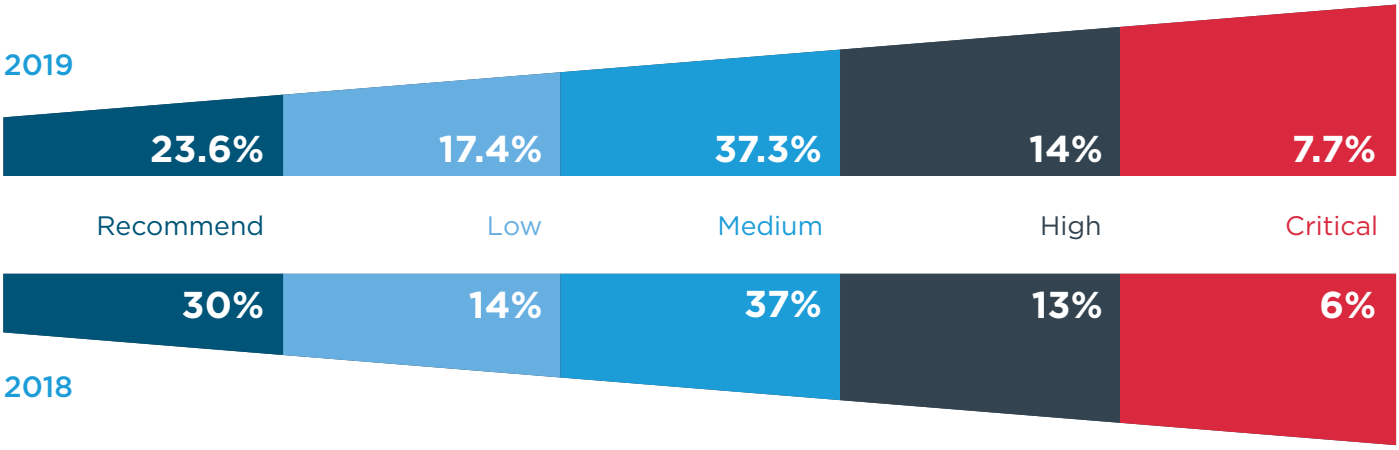
Selling personal information on the dark web

Ransomware

Cryptomining

VULNERABILITY BREAKDOWN

We've broken down customer vulnerabilities by severity to assist them in prioritising remediation as organisations don't often have the resources to fix each issue immediately.

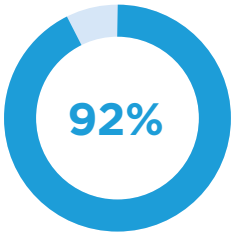


74% of businesses feel they lack the right cyber security personnel.

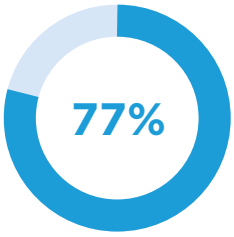
COMPANIES WE TESTED FAILING ON GDPR

Working closely with our customers we've identified 3 core areas where organisations are challenged in meeting the GDPR requirements.

Data Protection Principles



Ineffective DPIAs



Individual's rights

THOUGHTS FROM OUR HEAD OF PEN TESTING

New exploits, methods and technology are emerging all the time

A good penetration tester has to be part **cutting-edge researcher** and part **technical historian**.

Penetration testing is an intriguing business. New exploits, methods and technology that leave environments or apps vulnerable are emerging all the time. It's clear that old vulnerabilities and exploits never completely go away.

Web application development has changed a lot over the last few years and there has been a steep rise in the number of applications per organisation. The days of custom web applications are mostly gone, with modern applications tending to be built from existing frameworks that, generally speaking, are far more secure out of the box. Building a secure application used to require highly skilled developers, meaning the more complex the application, the more expensive it would become. So, it comes as no surprise that efforts have been focussed on trying to produce frameworks that simplify app building and make it easier and cheaper to secure them.

To a certain extent, this has been successful. Companies can produce apps on a budget and these apps (in theory) should be relatively secure. However, the downside to this is two-fold. One issue is that any new vulnerabilities that come to light within a specific framework affects a large number of companies, not just one. The other, is that a considerable number of organisations rely on third-party libraries.

WordPress currently runs around 30% of websites[1] and have stated that they aim to eventually run 80%. One platform running 80% of the Internet has an obvious problem. If a flaw is found within their platform, it will suddenly be present in 80% of all websites. What's more, there are plug-ins to consider. Plug-ins can introduce flaws into a website and popular ones end up in thousands of sites. It's estimated that 98%[2] of WordPress vulnerabilities were due to plug-ins.

Despite businesses having a new-found ability to create apps easily and efficiently, there doesn't appear to be a decline in the number of application bugs being discovered. Similarly, the number of high and critical issues appearing in the wild has remained relatively stable. Of course, this comes down to a number of different factors. Services still running on legacy apps contribute to a large number of vulnerabilities affecting companies, and the aforementioned reliance on third-party libraries is becoming more of a pressing issue. It's not to say that these libraries are inherently more flawed than anything that came before. In fact, there's an argument to be made that open-source libraries are more secure[3]. Still, if a flawed piece of code is used by hundreds or thousands of developers, then that flaw will exist in hundreds or thousands of applications.

The number of **application bugs** doesn't appear to be declining.

Ultimately, it is the arms race between the attacker and the defender that keeps us from being completely cyber secure. In some instances, it could be argued that a competent hacker is likely to have more experience and knowledge regarding cyber security issues than the average IT team. Whilst there are ways to proactively approach security, more often than not, it is a reactive role.

For example, 2019 saw the discovery of BlueKeep, a flaw that allows the possibility of remote code execution. This vulnerability affected newer versions of Windows, including Windows 10. The flaw, presumably, had always been there, it just had yet to be discovered. There are ways to defend against these, but they all rely on skills and expertise and companies have to have a reliable, proactive monitoring approach. However, this is an added cost that many small businesses would rather do without.

2019 saw the **discovery of BlueKeep**, a flaw that allows the possibility of remote code execution.

Unfortunately, if hackers uncover a flaw, they're unlikely to advertise it until they've monetised it as much as they can. It tends to be following breaches that these sorts of flaws come to light.

Whilst zero-days are often discovered by security researchers, there's no guarantee that they weren't already known to the hacker community or nation states.

In some respects, the idea of companies using simple third-party frameworks to produce applications is a good one. However, it relies on third parties diligently following best practices and implementing a reliable patching schedule as well as companies ensuring they are using the correct configurations and settings.

Unfortunately, as will become clear in our report, it's common for companies to still be struggling with very basic issues. When I first started working as a penetration tester over eight years ago, it was fairly common to be dropped into a network as part of an internal infrastructure assessment and have Domain Administrator credentials within fifteen minutes or so, due to a lack of OS-level patching. Whilst OS-level patching has generally improved over the years, lots of companies are still lacking an effective patching policy.

Kieran Roberts
Head of Penetration Testing

1 https://venturebeat.com/2018/03/05/wordpress-now-powers-30-of-websites/
2 https://solutionsreview.com/security-information-event-management/by-the-numbers-web-application-security-vulnerabilities/
3 https://www.darkreading.com/edge/theedge/the-truth-about-vulnerabilities-in-open-source-code/b/d-id/1335187

EXPLOITING WEAKNESSES: OUR PENETRATION TESTS

Throughout 2019 our penetration testing team conducted hundreds of tests, including application, infrastructure, API, mobile and even hardware tests. They also conducted numerous successful social engineering campaigns.

Interestingly, 20% of tests conducted featured a critical-risk issue. We define a critical risk as 'an issue which poses an immediate and direct risk to a business.' For example, using default admin credentials on a component can be considered a critical risk, as it would allow hackers to gain access to important parts of an infrastructure with admin-level privileges.

Such a risk leaves sensitive information vulnerable and will lead to a breach or the installation of malware if not remediated.

36% of our tests contained high-risk issues. Whilst not as immediately alarming as critical flaws, these still pose a significant risk.

These issues will not necessarily require a lot of skill or time to exploit and, even if they did, there are plenty of skilled hackers lurking in the wild.

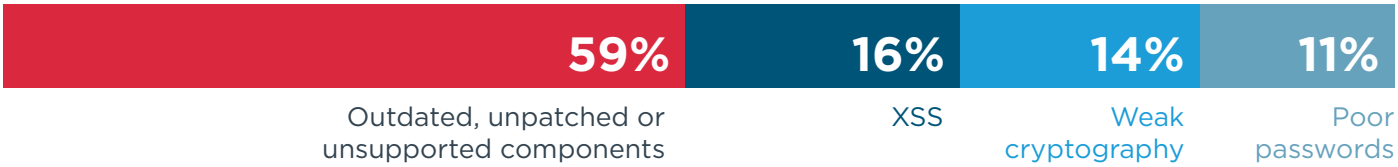
It's startling to see that **1 in 5 companies** tested have critical flaws present in their applications or environments.

Of all the high and critical flaws, the top recurring were:

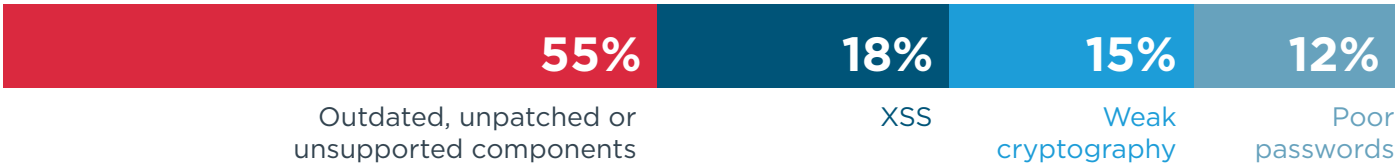
TOP RISKS 2019

For the most part, this is relatively consistent with previous years:

TOP RISKS 2018



TOP RISKS 2017



The top offender is once again the use of **outdated** or **unsupported components** and software.

WHAT THE NUMBERS TELL US

The only notable change is the drop off in cross-site scripting flaws (XSS) and the rise of access control issues. A lot of separate issues can fall under the umbrella of 'access control'. The simplest example would be 'www.examplepage.com/admin' being accessible to users who shouldn't have access. These sorts of flaws are many and varied and all present different risks to data.

The top offender is once again the use of outdated or unsupported components and software. Exploiting outdated software is often the easiest way to compromise a network. Patches are usually released to rectify security issues and should be installed as soon as they are available.

It's worth noting that these top offenders – outdated software, weak cryptography and poor passwords – illustrate that businesses are struggling to maintain best practices. For example, a regular and reliable patching schedule would go some-way to solve the outdated software issue.

WHY GETTING THE BASICS RIGHT IS HARD

First and foremost, environments are getting more complex and including more applications. If businesses haven't been keeping their asset inventory up to date (another best practice) it can be difficult to tell what is currently running and where[4]. These often-sprawling environments also mean simply patching everything all the time isn't always effective. Ideally, patches need to be tested to ensure the update doesn't have a negative impact elsewhere, which may have serious consequences. Unfortunately, running patches in a test environment before rolling them out to live can be resource intensive. It costs money, time and staff, which presents another challenge.

A growing number of businesses are relying on third parties for at least part of their service. Hosting, for example, would have been an in-house job a few years ago, but now, many businesses are moving towards cloud-based hosting providers. In such situations, ownership can be confusing and where the responsibility for patching lies can be up for debate.

If you don't own the asset, you can't necessarily install updates. Then of course, there's human error, which can be particularly prevalent with complex environments. Mistakes can be made, leading to more pain, particularly for small businesses who might not have the right expertise.

Ownership can be confusing and where the **responsibility for patching lies** can be up for debate.

Our penetration testers see a variation in their tests in terms of outdated software. One observation made by all is that, when conducting internal tests, 80% of unpatched systems relate to Microsoft patches. What's more, in these instances, they tend to be very out of date.

4 https://www.ncsc.gov.uk/blog-post/the-problems-with-patching

In terms of why this is, some organisations are just unaware that they need to be patching. Others are worried patching will cause errors elsewhere and underestimate the risk they are putting themselves in.

Another observation made by one of our testers is that "externally speaking, there has been some improvement, mainly due to new technologies and the adoption of cloud services, along with an element of heightened awareness. However, internally it's the same mess."

With all this in mind, it's unlikely that we'll see this issue ever go away. Ideally, we would like to see this reduce. With more compliance schemes gaining popularity (such as Cyber Essentials), adhering to best practices is becoming more of the norm. In essence, this works by introducing a model that enforces the best practices that are easiest to achieve. Once businesses have managed these, expanding into others becomes more feasible.

WEAK PASSWORDS

Default or weak passwords is another old issue. Again, particularly with default admin credentials, this is often down to simple oversight. Storing passwords in plain text or a poor password policy is once again running against best practices.

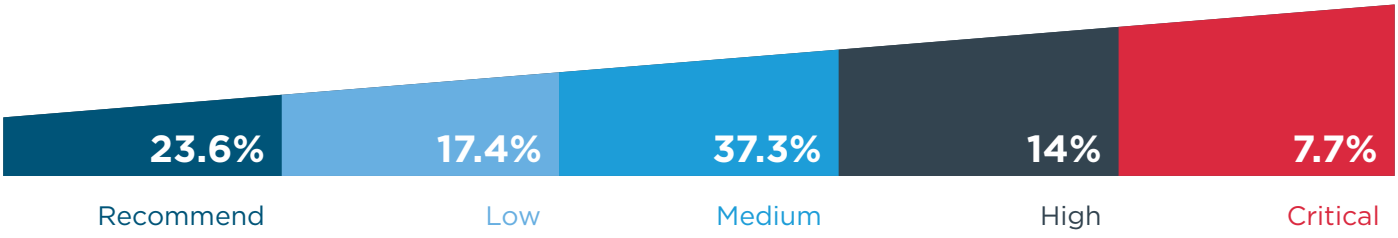
WEAK CRYPTOGRAPHY

The use of weak cryptography is often down to a configuration setting and is easily remedied. On the whole, we find clients aren't even aware they're using outdated cryptography. Whilst it is harder to exploit cryptography issues than leveraging outdated components, it's still a dangerous flaw to have, particularly if sensitive information is involved.

BREAKING DOWN THE WEAKNESSES

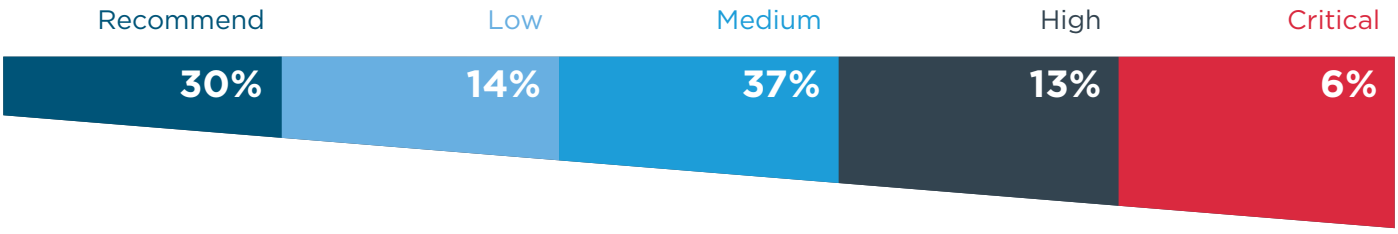
Throughout 2019, we discovered thousands of flaws varying in severity. These are broken down as thus:

VULNERABILITY BREAKDOWN 2019



Percentage wise, there isn't much variance from 2018:

VULNERABILITY BREAKDOWN 2018



What's immediately striking about both sets of results is the proportion of medium-risk issues in comparison with low risks. There's no definitive answer as to why this is, but the key takeaway is that businesses aren't getting better at securing their environments. Whilst not as immediately alarming as a high or a critical, a medium risk is still a danger, especially if more than one exists in a single environment. A skilled hacker can chain attacks together to exploit medium-risk flaws to gain access and compromise a network. For example, the below shows the approach a hacker might take to exploit multiple medium risks:

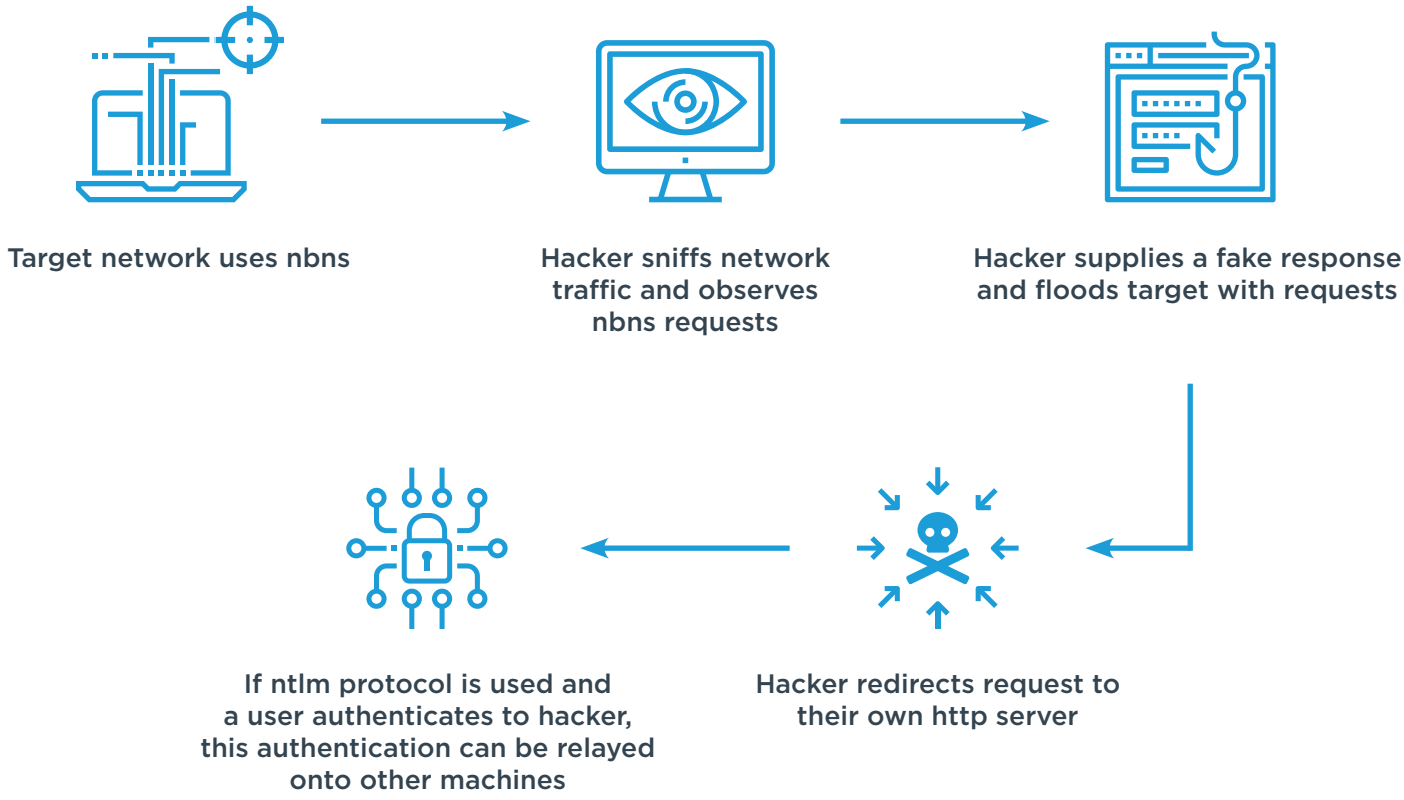


Figure: Chaining attacks together

This attack relies on exploiting a number of flaws. At the end of this, hackers could potentially escalate their privileges.

NAME AND SHAME – MOST HIT INDUSTRIES

On an industry-wide level, the most targeted industries[5] are:

19% Finance & Insurance

13% Transportation Services

12% Professional Services

11% Retail

10% Manufacturing

5 https://www.makeuk.org/insights/publications/2019/09/06/ cyber-security-and-manufacturing

We have broken our results on targeted industries down via severity of flaws found:

CRITICAL

In terms of critical flaws (the aforementioned outdated software or use of vulnerable components), the worst offenders with joint 18.5% of such flaws, were the education, construction and automotive industries.

18.5% Outdated software
Education, construction and automotive

15% Sensitive information disclosure
IT

14% Weak encryption
IT, healthcare, marketing, entertainment and leisure and insurance

HIGH

Industries with the most highs (again outdated components) were entertainment and leisure and healthcare, with 17% and 10% of the flaws respectively.

MEDIUM

Weak encryption and ciphers were big offenders for medium risks. With IT, healthcare, marketing, entertainment & leisure and insurance industries all sharing 14% of these flaws. This is closely followed by information disclosure issues. Retail and marketing both contained 15% of such flaws.

LOW

Sensitive information disclosure was the most common low-risk flaw. IT companies provided 15% of these findings.

It's fair to say there will be a lot of variation within each individual sector and one education establishment will have a better security posture than another. As to why education appears to have so many critical flaws, we can only speculate. The most likely explanation is one of budget and lack of knowledgeable staff.

The more flaws, the bigger the risk

The less time and effort it takes to compromise an app or infrastructure, the more profitable a hack can be. If there are vulnerable components in place in a network or application, it's likely it will be hacked.

Getting the basics right lays down strong foundations for incorporating security by design. The idea being that security is considered at every stage of development, rather than an afterthought.

LEVERAGING THE HUMAN ELEMENT

Social engineering can be the easiest way for a hacker to compromise a network. In 2018, a third of all reported data breaches was due to phishing[6].

Phishing is a concept everyone will have experienced at some point, even if they didn't know what it was called. It is the attempt to leverage the human element of a business with a malicious email, either to obtain credentials or financial details, or trick the user into downloading and installing malware.

Of course, phishing isn't solely done via email. In Q2 of 2019, there were roughly 182,465 phishing websites[7] active. Social engineers are quick to jump on big brands, particularly in the event of a product launch. For example, in March, Apple launched a new product and subsequently the number of Apple imitation sites peaked at 79,936[8].

In Q2 of 2019, there were roughly **182,465 phishing websites**[7].

WHY CONDUCT A PHISHING CAMPAIGN?

Users are one of the biggest threats to an organisation. Even with the best security tech in place, you can be breached by an unwitting member of staff. Hackers are aware of this weakness and work hard to exploit it. Research suggests that roughly 3.4 billion phishing emails are sent daily[9].

As external defences get better at keeping hackers out, the user becomes the path of least resistance. If members of staff don't know the tell-tale signs of a phishing campaign, then your business is as risk.

GETTING THE MOST OUT OF YOUR PHISHING CAMPAIGN

Crafting an obvious phishing email that everyone will spot doesn't offer much value and neither does creating a campaign that will fool everyone. Before starting a campaign, we always work with our clients to find out what they want to achieve. Are they testing their responses to external communications or internal? Do they want us to obtain credentials or get users to open a document? A blanket approach to a preselected number of individuals often yields the best results.

3.4 billion phishing emails are sent daily[9].

The best approach is to send a tailored email to a randomly selected group of individuals across a number of different departments. It's worth getting some spoof login portals produced to make a campaign more convincing. In many Bulletproof phishing campaigns, we have crafted an email that offers targets an employee perk, as users are more likely to click a link if they think there's something to gain.

COMMON THINGS TO LOOK OUT FOR IN A PHISHING ATTEMPT

- **Dropping in a logo** is common practice
- **Spelling errors** are common in phishing emails
- If they cannot spoof the sender address, hackers will register a domain that, at first glance, **looks like a trusted sender**
- **Poor grammar/misleading words** are common

6 https://www.thesslstore.com/blog/20-phishing-statistics-to-keep-you-from-getting-hooked-in-2019/
7 https://www.statista.com/statistics/266155/number-of-phishing-domain-names-worldwide/
8 https://securelist.com/spam-and-phishing-in-q1 2019/90795/
9 https://www.techrepublic.com/article/more-than-3b-fake-emails-sent-daily-as-phishing-attacks-persist/

PROTECTING BUSINESSES 24/7

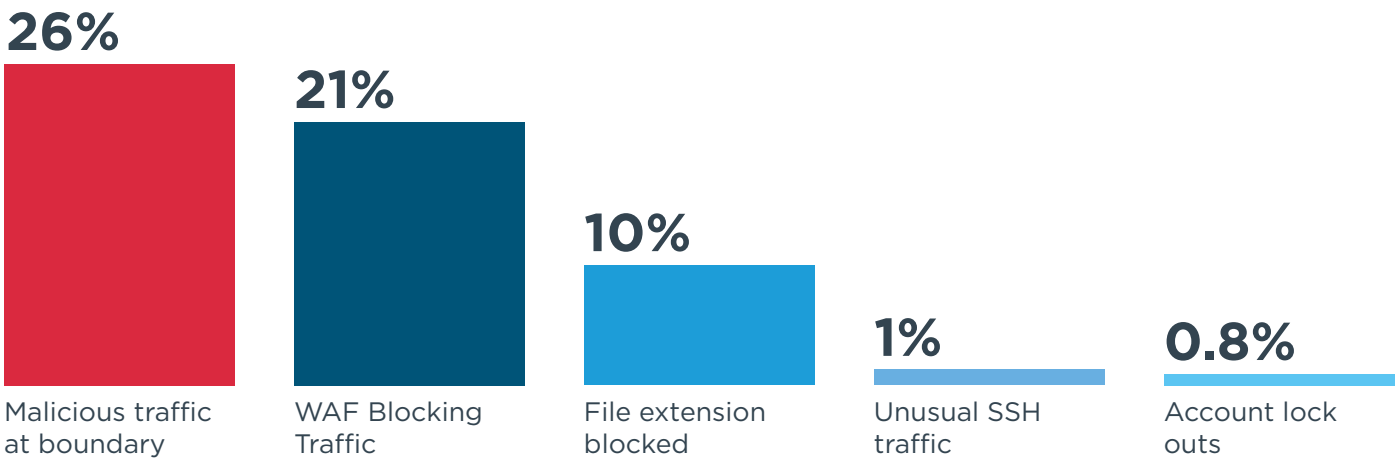
An increased awareness of cyber security and an uptake in compliance packages has put greater emphasis on the importance of active monitoring. 2019 saw the release of our S.W.A.T. Defence® service. Building on our existing SIEM platform and SOC, S.W.A.T. Defence® combines cutting edge SIEM technology with active threat hunting from experienced analysts.

SIEM technology has been around for years, but it's only recently that businesses have really started to treat them seriously. Numerous compliance packages make log monitoring mandatory, which is certainly one driving factor. Also, the technology and approach has drastically improved over the years. If an organisation is monitoring their environment effectively and taking the appropriate action, the risk of a breach is drastically reduced.

S.W.A.T. DEFENCE® IN ACTION

On average, our SOC was processing 15,000 events per second and billions of logs every month. Throughout the year we saw 1.8 billion Windows events alone. We raised 675 events that required action and 975 that were determined to be a 'security event'.

The top offenders for security events were:



MALICIOUS TRAFFIC AT THE BOUNDARY

As seen, malicious traffic at the boundary is one of the most common threats facing organisations. It's a high-level term and we can break this down into more meaningful data by looking up the specific activity that triggered these events.

The most common cause of these comes from the Intrusion Detection Systems (IDS) that we monitor for our customers. On average we see around 120 IDS alerts a month, the majority of which can be attributed to one of three main alerts:


SMTP Command Injection Attacks


Web PHP Injection Attacks


IP/Port Scanning

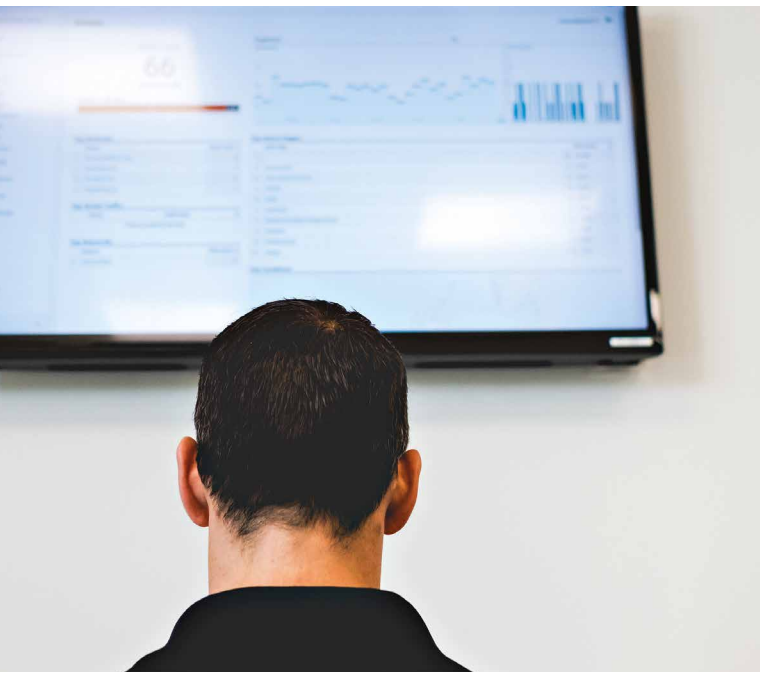
WHAT OUR SOC DATA REVEALS

Looking at the data, the attackers continue to rely on the same approach that works. This is unlikely to ever go away.

Whilst it's important for businesses to be made aware of these bad actors, so that they can be blacklisted, it's well known that hackers can simply switch to another IP and try again. This is why it comes as no surprise that malicious access attempts to customer networks are the most common security events.

Tracking of these events allows analysts to begin to predict what activity may come next. Attackers will often work their way through a range of IP addresses. Analysts can predict this pattern if the initial incidents are highlighted and investigated early enough. Malicious access attempts cover a wide variety of malicious traffic, which can include application or port scanning, Geo-IP specific incidents and brute-force attempts. With the increase in cloud computing, organisations are able to access their networks from practically anywhere in the world, which has led to a rise in attacks being made against the boundary.

Analysts can predict patterns if the initial incidents are highlighted and investigated early enough.



WAF BLOCKING TRAFFIC

(Web Application Firewall) WAF blocking traffic might seem like a good thing at first. If the firewall is blocking traffic, then surely it is doing its job. However, it's a bit more complicated than that. This blocked traffic is indicative of someone trying to do something that they shouldn't be. It may be a sign of a wider on-going problem, which can sometimes require further investigation.

If you were to look at the cyber kill chain and apply it here for example, a firewall blocking traffic could indicate a hacker is at the 'action on objectives' stage of an incident, which would indicate that a host has already been compromised. It's important to investigate other surrounding information to get a true reading on the importance of a single event.

BLOCKED FILE EXTENSIONS

Blocked file extensions can relate to a number of different things, such as inbound emails sporting an attachment that is not allowed. These could be indicative of blocked phishing emails, or even a user sending a document that, unknown to them, is malicious. More worryingly, it could be a sign of someone attempting to exfiltrate data. Clients need to be informed of this activity, just in case it is being blocked unnecessarily and preventing legitimate traffic from getting through.

Insider threats are still one of the biggest risks to an organisation. An insider can easily undo any security features you have in place. An event flagged concerning a genuine user attempting to exfiltrate data will often be classified as an accident. Companies will simply accept that the activity was blocked and not investigate further, which can be to their detriment if the account is in fact compromised, or the user is up to no good.

SSH TRAFFIC – HAVE YOU BEEN COMPROMISED?

Servers running SSH are a constant target and there are plenty of known SSH vulnerabilities that hackers can exploit, so these should be monitored closely. This is where a 24/7 SOC is necessary, as seeing this activity at, say 00:00, would seem very suspicious and require immediate action.

Account lock outs might seem relatively benign, but it could be a sign of someone attempting to brute force an account and subsequently locking it out. If this is the case, some investigation work will need to be done and the offending IPs blocked.

MALICIOUS OR NOT? ONLY INVESTIGATING WILL TELL

All of the above-mentioned alerts may seem benign when only a single occurrence is seen on the network. They may end up being misclassified as a false positive under the assumption that the firewall was simply doing its job. A blocked file extension might be seen as an "accidental" attempt to email out a .zip file to their personal address. This mind-set is rather dangerous, and it's always best to treat a single event with suspicion and not immediately discount it as a false positive. Investigate all other activity relating to the event wherever possible. This is key to uncovering other suspicious actions that may be related or have occurred elsewhere.

If a firewall is blocking activity, it becomes necessary to check for other indications of compromise (IOCs). Is this the first time the activity has been seen? Have any changes been made to the internal host recently? Has a new user logged into the host recently? Etc. All of these checks can help an organisation confirm if said activity is indeed a single event or if it is part of something more serious. All it takes is one analyst to spot one instance of suspicious activity and a malicious user's presence can be discovered, no matter how well they've covered their tracks.

Unfortunately, this is often not possible for a lot of companies, particularly smaller ones. Those with tighter budgets and smaller teams are unlikely to have the resources to conduct these sorts of investigations as and when they happen, meaning they're often left open to risk.

Is this the first time **the activity has been seen**? Have any changes been made to the internal host? Has **a new user logged** into the host?

USER ACTIVITY: THE BIGGEST THREAT

With users often being the path of least resistance, it is critical that organisations observe the early signs of attack and monitor for account compromise events. Due to the nature of user activity in organisations, the ability to detect these activities is challenging. It is important to focus on specific events and perform threat hunting based on intelligence and being smart about proactive monitoring. There are common events to look out for, such as 'Firewall Configuration Change'. A lot of the time this turns out not to be malicious, but this is an indicator which shouldn't just be ignored. Such changes may put your business at risk, whether that was the intent of the user or not.

Malicious users may look to extend access beyond what they currently have. Bad security practices could lead to standard users having access to folders they shouldn't. Equally, users might be created with higher levels than their role requires, meaning they can make changes unchecked or cause accidental damage, such as running malicious files as an admin, or deleting important files.

It is important to focus on **specific events** and **perform threat hunting** based on intelligence and being smart about **proactive monitoring**.

THE THREAT FROM WITHIN

The majority of our events (roughly 53%) relates to user activity, with spikes predictably seen between 8 and 11 am, with another spike in the afternoon. This relates to log on activity. A targeted attacker may choose these periods to hide in plain sight.

It's important to monitor such activity as it's the best way to spot early signs of compromise, with particular emphasis on:

- Command and control activity
- Files being dropped post compromise
- Administrator account compromise
- Vulnerabilities detected
- Phishing attacks

Strange user activity, such as obscure login times, staff accessing folders they shouldn't be or logging in from unusual location etc. can often lead to false positives. We still see numerous instances of users running service accounts under their normal domain account or regular users with admin privileges as well as test accounts being used for day to day activity, not removed or disabled after use. Similarly, we see people using admin accounts when they should be using their regular user account.

Whilst it may seem pedantic, the danger of accidental damage through use of admin accounts cannot be understated. This, combined with changes being made to environments without the correct notification processes being followed, can play havoc with alerting and auditing. In a forensics investigation, we discovered a user with admin privileges was accidentally responsible for initiating a dropper file, which in turn led to a ransomware outbreak across their network.

53% of events are related to user activity.

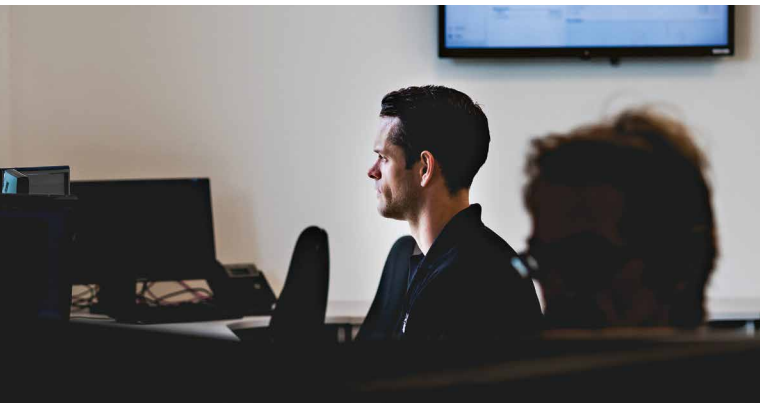
Having so much user activity to monitor is both a gift and a curse. As users are still one of the biggest threats to security (with 99% of attacks requiring human interaction[10]), it's good to see that we're able to record this information and that businesses are willing to record it. It shows they are aware of the risk and are taking it seriously. However, there's so much user activity that it can often obscure other things.

DANGERS OF MOVING TO CLOUD SERVICES

Response to unusual user activity needs to be quick. Hackers regularly seek to use compromised user accounts to gain access to a network. It's just as important to monitor user activity as more businesses move towards cloud services. We have seen several large data breaches over the last year or two which have provided the hacking community with several large data dumps. Some of the largest contained more than 700 million records.

What does this mean if you are in the cloud? The same as if you use a traditional solution. Hackers use techniques such as credential stuffing and spray attacks that prey on one of the most common human traits and weaknesses, reusing a password. This has been exacerbated by large scale data breaches where attackers have gathered a huge list of breached accounts from the dark web and are now trying the credentials against a whole slew of services and sites exposed to the Internet.

In opportunistic attacks, an attacker can simply get lucky using this technique. A targeted attacker would still use the data in the same way but typically with a different frequency. In addition to this, although many organisations now trust third parties to provide core parts of their infrastructure, moving to the cloud has changed many organisations' visibility. A lot of people simply lack the expertise when it comes to monitoring these platforms, as they do not have a way to get the data into their monitoring systems, or the package they have purchased does not include the tools to conduct a thorough investigation. Also, many employees have not been provided training around cloud environments or other new technologies.



10 https://www.techradar.com/news/people-are-still-the-biggest-security-threat

OFFICE 365: A FALSE SENSE OF SECURITY

Too often, organisations move to the cloud assuming it is safer, but forget there is a shared responsibility model and they still need to do a lot to secure it. Take Office 365 for instance. More and more businesses are opting to use it and some wrongly seem to be under the impression that it is innately 'unhackable', without adding their own layers of security. This is sadly not the case and can lull people into a false sense of security and then to complacency. We still see brute-force attempts and credential stuffing, which has likely contributed to this being a more prominent attack vector. It's a simpler approach, making hackers less likely to opt for more complicated methods such as exploiting outdated software. The right logs will often show people attempting to access the domain, but using the wrong email formats, trying to see what works, providing the opportunity to take action before the issue escalates.

WHO'S TRYING TO LOG IN?

O365 is a honeypot in its own right. Just like everyone else, Bulletproof is a target, perhaps quite an enticing one too. We regularly see attempts to log into Office 365 using Bulletproof accounts. One such instance involved our co-founder Oliver Pinson-Roxburgh attempting to log in from China. This might not seem suspicious, as directors are often required to login abroad. However, Oliver was sat in our Hertfordshire office at the time, which was enough for us to deem this activity suspicious.

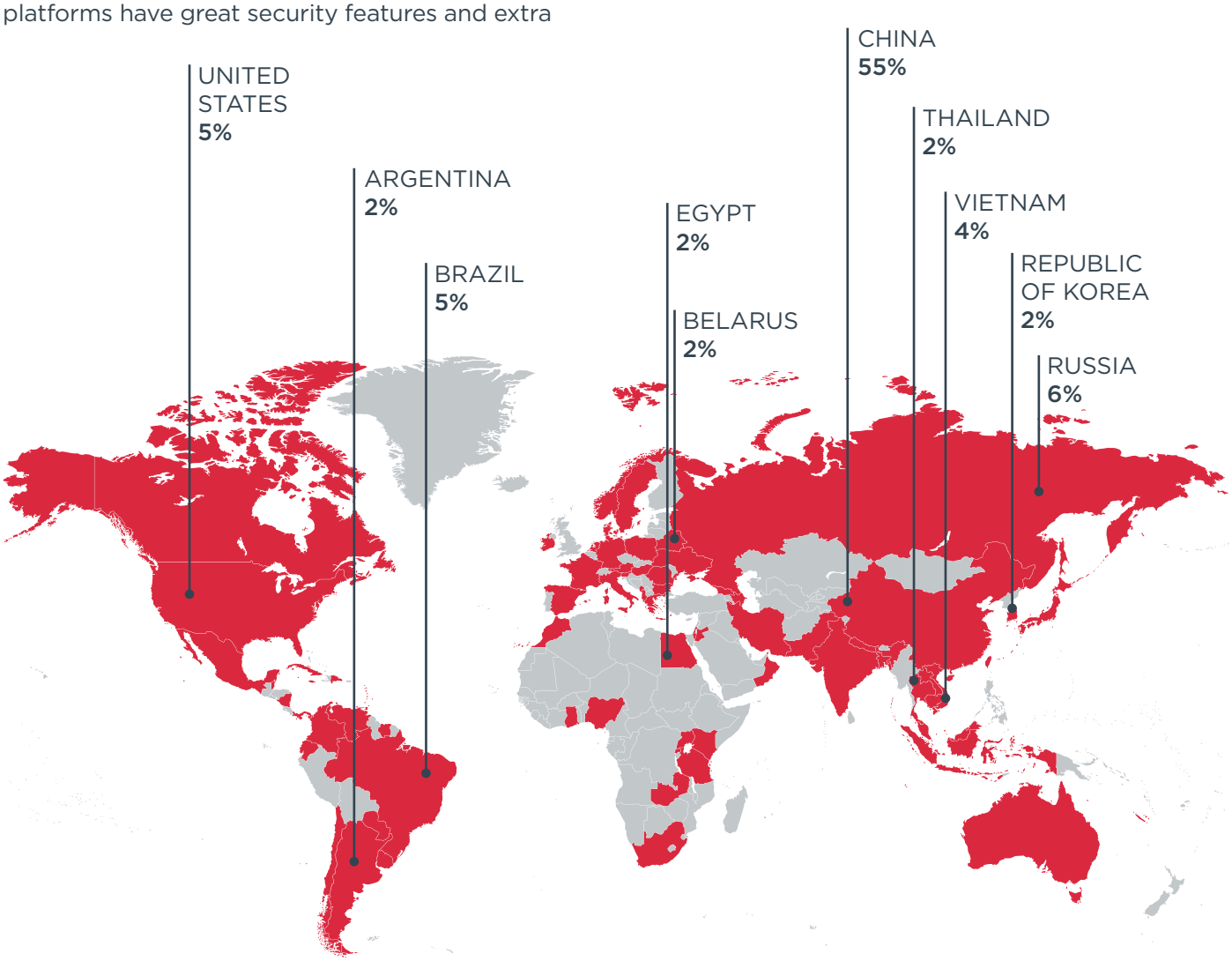
The most likely scenario is that these would-be hackers had found our co-founder's name online, after all, we have not kept it a secret. Using that name, they would have tried to brute force his Office 365 login. Obviously, we have extra layers of security preventing unauthorised logins such as 2FA as well as constant monitoring. But this was not an isolated incident.

A small business can expect **over 4,000 malicious logins** in a month.

In fact, in one month we saw over 4,000 failed login attempts, the majority of which were not even from Bulletproof users. These came from 39 real usernames and 14 false ones. Whilst some of the failures would be from people accidentally mistyping their passwords, it is highly unlikely that these had a huge impact on the thousands of failed attempts.

As the year went on this rapidly went down until October when we were seeing 610 login attempts. However, the number of fake users had gone up to 120. This shows that cloud environments are not necessarily hardened and can still be bruteforced. Most businesses would be none the wiser if they were compromised this way. Whilst many cloud platforms have great security features and extra layers such as 2FA are provided and encouraged, many companies are still treating security as an afterthought.

These login attempts came from all over the world. Countries observed with the highest activity are marked below:



A total of 87 offending IPs were known bad actors (KBAs). All offending IPs were added to our blacklist.

NOTHING IS INNATELY SECURE

The above demonstrates that nothing is innately secure, which is the mindset of many businesses moving towards cloud services. There's also the misconception that security issues are the responsibility of the third party. The truth is there is a shared responsibility and organisations must incorporate settings and monitoring solutions to ensure their services remain as secure as possible.

THREATS ARE NOT ALWAYS FROM HACKERS

For a clearer view into the day-to-day activities of a SOC analyst, here is a real example of an investigation into a potential threat.

Midway through the year, a client was concerned by a number of alerts being raised by their IDS. The alert claimed a host was attempting an attack using Google Golang (a programming language) which suggested that a host had been compromised. After some preliminary investigation work, we concluded that this was a false positive. However, over a number of days this alert kept on appearing. The client, understandably, grew concerned. To reassure them, it seemed some serious investigation work was in order.

The IP address associated with the 'attack' was linked to the client's guest network. Using the MAC address of the host, we inferred it was likely coming from an Apple device. After investigating the activity from this MAC address and comparing it to the logs, it showed web browsing activity, specifically visiting the client's website. After a little more digging, we discovered the IDS alert was being triggered by a named iPhone. The name revealed that this activity was coming from a member of the customer's underwriting team. As the alerts were being generated as a result of simple browsing, and nothing else concerning this phone was deemed malicious, we were able to confirm it was indeed a false positive.

You may be thinking at this stage 'all this effort for a false positive?' However, as we knew what to look for and were quite sure what was happening, this didn't take long at all. As we had the right log information and meta-data, we knew where to look. The whole investigation amounted to an hour and a half, which is very quick for an investigation of this type.

Imagine being faced with the same ominous alert but relying on your busy IT team to investigate. More worryingly, some businesses would not be recording this information and would therefore be unaware of any issue. If this was a real security event involving a compromised asset, a hacker would have had access to data until it was discovered – perhaps by chance.

THE DANGERS OF DWELL TIME

The aforementioned investigation operates as the perfect case study showing the importance of collecting, monitoring and investigating the right logs. Had it been an actual attack and not a false positive, and had the business not been collecting the right logs, then they would have been vulnerable. A hacker could have compromised the network and the business would not have been aware.

Dwell time is a serious issue in cyber security. It is the length of time a breach or malware goes undiscovered. The longer a hacker has access to a system, the more damage can be done. If you're not monitoring the right things and collecting the right data, dwell time can increase exponentially. SMBs are particularly vulnerable to lengthy periods of dwell time, especially if they don't have any monitoring in place. However, big companies are not immune to expansive dwell times. Big names are compromised all the time, and many don't realise it for months.

The key to reducing dwell time or avoiding it entirely lies in capturing the correct types of data and meta-data. Often, an attacker needs to install tools or initiate a connection which will seem abnormal on a given environment. Observing strange files being created, or new, unexpected processes are clear early signs of a breach.

Intelligence feeds can be used to automatically prevent a lot of attacks. New vulnerabilities tend to be well defined when they reach the public. This sort of intelligence can inform detection rules. Another approach is to start threat hunting.

The longer a hacker has **access to a system**, the more damage can be done.

INFORMATION IS VITAL, KNOWLEDGE MORE SO

Many of the issues observed through our research suggests that, for most businesses, the lack of specialist knowledge and the failure to capture the relevant logs in a central repository leads to investigations taking days, or weeks. Bulletproof are often called upon to conduct forensics investigation only for us to find that the relevant log files haven't been collected, giving us little to go on.

When it comes to a breach, or the possibility of an ongoing event, businesses often act out of panic. More often than not, this leads to rash decisions or worse, indecision. The key here is to have a well-defined and tested incident response plan.

False positives are just a fact of cyber security. They will never go away and nor should they. If false positives aren't investigated, there's a risk you'll miss something big. Of course, you don't want too many false positives, but if you aren't getting any, it suggests your security strategy isn't particularly thorough.

False positives can be a struggle for many businesses. Particularly if they come at the end of a time-consuming investigation. They can feel like a drain on resources, both time and staff power. They can reduce faith in security products or, as a result of too many false positives, real attacks fly under the radar. This is something hackers have exploited in the past, using DDoS attacks as a smoke screen to distract security services from data exfiltration.

HUMAN ERROR IN THE CLOUD

As already discussed, more and more businesses are turning to the cloud. Amazon S3 buckets allow businesses to store and retrieve data from anywhere in the world at any time. They are incredibly useful and convenient allowing up to 5TB of data on each one.

On the whole, Amazon is quite stringent on security, but they make it clear that it is a joint responsibility. You'd be wrong to assume that your buckets are secure 'out of the box'. You have to do your own monitoring on them and limit access according to the need.

THREAT DATA

Our SOC is fed with up-to-date threat intelligence, taken from a variety of different places. We have developed a new platform to feed it with even richer data in a bid to further automate aspects of threat hunting and crowd sourced intelligence gathering.

The quality of threat intelligence is integral to a good security practice. If it's not updated on a regular basis or only pulling information from one area, then it is unlikely to be effective. The key is getting as much trusted data as possible from different sectors and locations.

KEY TAKEAWAYS

Users represent a key threat to businesses either through deliberate or accidental action. A lot of user-associated risks are due to best practices not being followed, such as user accounts with higher privileges than they require, or user accounts being used as service accounts etc.

The amount of malicious traffic hitting the boundary shows that businesses should be monitoring their environment 24/7. Threats can come from anywhere at any time, so unless they have adequate monitoring in place, they will go unnoticed until it is too late. This is rapidly becoming a full-time job in itself, as a knowledgeable analyst needs to be available to action any and all threats raised by technology. Companies struggling with monitoring due to an over-abundance of false positives need to evaluate what it is they want to achieve and what assets need monitoring and what their users should be made aware of. It is likely they will see immediate benefit after some brief reconfigurations.

CASE STUDY:

ACCIDENTAL EXPOSURE

This year, we were called upon to investigate an incident whereby a customer accidentally leaked the keys and details of their S3 bucket by making them public on a user's Git repository. This particular bucket contained lots of data regarding their test environment. A large portion of a test environment makes it to their production deployment, so if hackers managed to get at this information, then they could theoretically have a working knowledge of what's running, what security is in place and, potentially, what flaws can be exploited.

Following this revelation, the keys were retracted and the access concerning this particular user temporarily revoked as Bulletproof assessed the environment to make sure these keys were not used during this period. Whilst conducting this investigation, we discovered details of another user had been exposed and informed the customer who promptly acted.

This is a good demonstration showing that the cloud is not inherently more secure than traditional environments and that effective monitoring needs to take place there too. It also demonstrates that simple mistakes can cause massive issues and processes are just as important in an agile ephemeral environment as it is in a more traditional static model.

PRIVACY BY DESIGN AND COMPLIANCE TRIALS

Whilst we've always said compliance does not equal security, it is an important part of a business's strategy. More organisations are looking to technology to automate a lot of their compliance and regulatory activity. Such technology (regtech) is expected to make up 32% of regulatory spending by 2020[12].

We've seen a rise in companies obtaining Cyber Essentials or Cyber Essentials Plus certifications, particularly in universities, which has seen as much as 40% of UK universities becoming Cyber Essentials certified[13].

Companies becoming **Cyber Essentials certified** has risen.

40% of UK universities are now Cyber Essentials certified.

Cyber Essentials is mandatory for government organisations and it may soon be mandatory to undergo a penetration test to gain certification. This government-backed scheme's main selling point is that it helps establish trust between a business and their customers. Ultimately, it ensures that the basic best practices are being followed in regard to cyber security. This is effectively the case for all compliance schemes, from PCI DSS to ISO 27001. They all ensure a set level of security is being maintained and ensures technical controls are in place.

We may see a change in the number of businesses providing Cyber Essentials and Cyber Essentials Plus services, as IASME has recently won the bid to become the leading authority. This means that all companies providing such services must apply to go through them. Currently, many companies providing Cyber Essentials consultancy do so through various other accreditation bodies, such as CREST, APMG International, IRM and QG.

The arrival of GDPR put a greater emphasis on privacy and laid out what companies can and cannot do with people's personal data. Much like how application developers – or infrastructure engineers – need to implement security by design, compliance and GDPR effectively pushes companies to incorporate privacy by design. A lot of companies we have provided GDPR gap analyses for failed in certain areas for not doing so.

GDPR – THE BIGGEST DATA PRIVACY SHAKEUP

There shouldn't be a single business that isn't aware of GDPR. Those four simple letters represented the biggest change in data privacy law since the Data Protection Act of the late 90s.

As it became fully enforceable in May 2018, the number of gap analyses we have provided, where we assess how close a business is to achieving full GDPR compliance, have predictably declined. That's not to say we haven't been busy on this front, not to mention (as a direct result of GDPR) our DPO service has gained a lot of traction. We predicted this decline last year as, naturally, businesses scrambled to get their affairs in order in the build up to that fateful date. Those that weren't ready by the 25th of May 2018 will have been gradually getting into a position where they can undertake a GDPR project. As the deadline has passed, there has been considerably less emphasis on the need to become GDPR compliant. There are still many companies struggling, however.

12 https://www.consultancy.uk/news/22261/the-growth-of-fintech-and-regtech-in-financial-services
13 https://www.ncsc.gov.uk/news/more-universities-strengthening-their-cyber-security

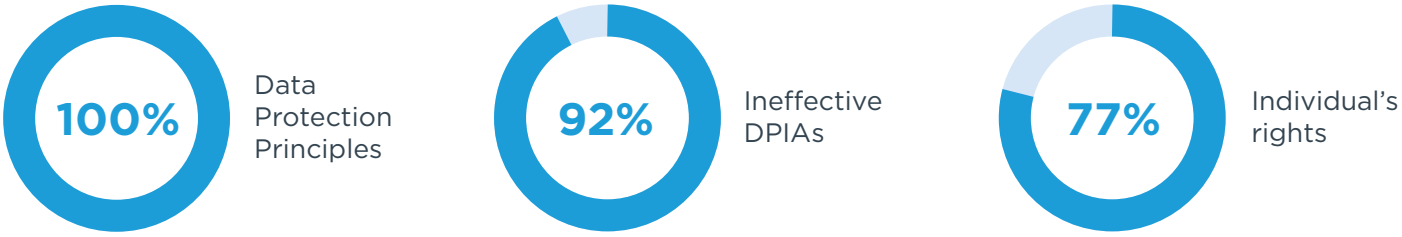
We were doing five times as many gap analyses in 2018 as 2019, which makes sense as there was a lot of noise around GDPR throughout the year.

There was also a lot of fear mongering in the build up to GDPR. The fact that regulatory bodies (ICO in the UK's case) could theoretically fine companies up to 4% of their global annual turnover was perhaps over reported. This no doubt had an impact on the number of companies looking to get compliant.

Our data shows that companies are still struggling to fully understand their responsibilities under GDPR. 100% of clients were deemed non-compliant in terms of Data Protection Principles, 77% failed under Individual's rights and 92% were not effectively conducting DPIAs or incorporating privacy by design. On a positive note, 100% were correctly obtaining consent from data subjects.

A lot of these issues are administrative and demonstrate that a lot of businesses aren't fully aware of the relevant data protection principles or haven't adequately assessed the risks posed to personal data. A lot of confusion comes from the fact that there are no set 'standards' so to speak that ensures GDPR compliance. There are different ways of going about it and a lot of companies don't know where to start.

COMPANIES FAILING ON GDPR



Source: Bulletproof customer data

Almost **500,000 DPOs** work in Europe.

THE RISE OF THE DPO

In 2017 the International Association of Privacy Professionals (IAPP) claimed that GDPR would create an estimated demand for Data Protection Officers (DPOs) of roughly 75,000 worldwide. More recent research suggests there's close to 500,000 DPOs already working in Europe alone[14]. Under GDPR, certain businesses have to have a DPO. Even if a business doesn't require a DPO, someone still needs to take responsibility for personal data. In our experience, we have found most companies opt for a DPO regardless.

On average, Small to Medium Businesses (SMBs) will need a DPO for what equates to one working day a month. This will translate to roughly 25 emails or calls a week. Some will require on-site engagement.

Organisations need to spend time assessing their business to work out how much contact time they will need. Two businesses of equal size may have different DPO requirements.

Businesses tend to struggle with subject access requests, which have become more prevalent as data subjects have become more aware of their rights. A lot of the issues come down to not understanding legal obligations or the correct wording of privacy notices.

Many businesses want someone to be accountable for any actions required on the data protection front and to be responsible for all related deliverables. Often, decision makers are under the impression that this is what a DPO is for, which it is not.

14 https://securityboulevard.com/2019/06/the-rise-of-the-data-protection-officer/

A DPO is in fact a protected position. It is their role to advise and oversee data protection is taken seriously and is in keeping with the relevant legal standards, not take sole responsibility for it or implement the controls themselves.

ISO 27001 OFTEN MISUNDERSTOOD

Too many organisations view ISO as an unachievable challenge that generates a lot of work across the business. This often comes down to a flawed approach that, in our view, is not pragmatic. It's important to remember the intent of the standard is to drive improvement where security is concerned as well as in regard to consideration of data and information. Businesses want this, but are often restricted by budget or staff constraints, and so opt not to become compliant, choosing instead to invest elsewhere to drive company growth.

We have seen a positive change in this, however. Partly driven by consumers and partly by suppliers there is a greater demand for compliance and more emphasis placed on security. ISO is slowly being viewed as an enabler rather than a drain.

In our experience, companies struggle with ISO 27001 primarily because they don't understand the requirements or controls. This is why a lot of people need the help of external consultants to guide them in the right direction.

Some of the key basic security checks which are often overlooked by businesses are:

Quarterly access control reviews

Quarterly firewall reviews

Monthly vulnerability scans on both the internal and external network

Lack of risk management framework

COMPLIANCE – PRIVACY BY DESIGN

High staff costs are said to be turning businesses towards technological solutions for much of their compliance responsibilities[15]. One of the biggest challenges with keeping up with compliance, as evidenced by GDPR, is change. As the threat landscape and technology changes, regulations change, and new compliance packages emerge.

There's a general misunderstanding of what goes into compliance and a misconception that a compliant business is suddenly unhackable. There is also a continued trend in the increase of 'compliance culture'. Compliance is becoming a big talking point and more companies appear to be taking compliance seriously.

Privacy by design needs to be more broadly understood by businesses and adopted as the norm for all projects. Existing projects need to be massaged into compliance retrospectively.

PAYMENT IS CHANGING. IS PCI DSS?

PCI DSS is aimed at protecting payment data and has remained relatively unchanged throughout the years. However, the way online payments are made have. Some of the most recent systems have started to move away from information being taken from the server side to client side, to where the browser sends the payment directly to the payment service providers.

This significantly reduces the risk of hackers stealing credit card data from vulnerable servers, which means they've had to update their approach. Of course, they have done just that. With the rise of e-commerce retailers, hackers discovered ways to swipe data from the client side via the use of scripts. This code is executed in a user's browser and steals information before it submitted to the service provider. It's a relatively stealthy approach that avoids detection from a lot of monitoring services.

15 https://www.forbes.com/sites/steveculp/2019/04/17/four-major-trends-for-compliance-professionals-in-2019/#694e11b467ad

How they get this code in place has also changed in recent years, in that hackers are writing JavaScript or using JavaScript files and dropping these into existing application code. One popular way of doing this is through open cloud services, such as Amazon S3, where they manipulate the JavaScript files in libraries hosted on insecure buckets. A small amount of code hidden in a larger collection of code can remain undetected for a long time. Developers are unlikely to spot it until customers start noticing something is amiss. Another method is to hack third-party providers, such as marketing agents or live chat sites – any way that lets people inject code into payment pages.

Even Level 1 PCI service providers have found themselves falling victim to skimming attacks.

Earlier in the year, Bulletproof conducted a forensics investigation where we found a relatively small amount of code is typically used for data theft. In some cases, it's as little as 20 lines. Hackers are usually pretty good at obfuscation too, which makes spotting these nefarious lines harder. Hackers will often disguise their code too, using naming conventions that one would expect in a website, such as Google's Gtag library.

This technique is called web skimming and has been very popular throughout 2019. Some of this year's largest hacks have used it, obtaining large amounts of information that was then seen on sale on the dark web. Interestingly, the code will often be included in organisations' internal systems, meaning that payment information in-putted over the phone could be taken too.

One of the biggest challenges is that the code is running on the browser side, so it is difficult for security tools to detect, as the server is not transmitting the traffic. Organisations need to focus on detecting attempts to include code into the application. Businesses can use content security policies (CSP) to prevent code being loaded from rogue sources and even use it to stop transmitting data to untrusted sources, but in our experience, most organisations don't have these controls in place.

Even Level 1 PCI service providers have found themselves falling victim to skimming attacks. The most obvious example being British Airlines who lost data belonging to hundreds of thousands of customers. Of course, following a forensics investigation the company was heavily fined, though it raises the question 'is PCI DSS still fit for purpose?'

It could be argued that having unnecessary scripts running on payment pages would be grounds for failure under PCI DSS. However, if this code comes about after a business has been deemed compliant and it isn't spotted, then the company will be in trouble. Code review is an element of PCI, but it seems this isn't necessarily being followed, or at least not regularly enough.

With thorough penetration tests, adequate monitoring – along with file integrity monitoring – and code reviews, you should be able to avoid this type of attack. Whilst compliance does not equal security, security does tend to equate to compliance.

BULLETPROOF INDUSTRY RESEARCH

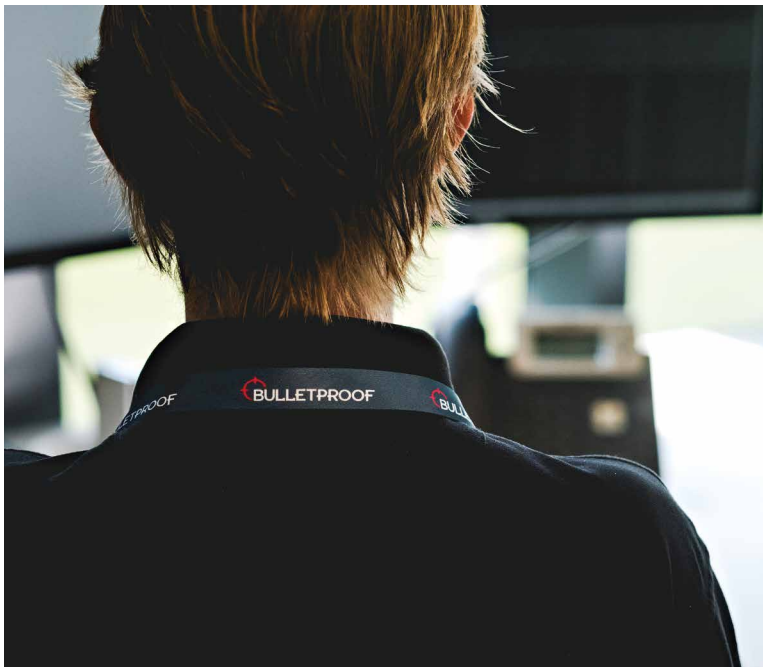
Almost every aspect of our lives seems to involve an online interaction of some type. It comes as no surprise that we are all more likely to experience being hacked then we are to experience a home invasion.[16]

According to NCSC's analysis of breached passwords the top 10 worst offenders were:

1. **123456**
2. **123456789**
3. **qwerty**
4. **password**
5. **111111**
6. **12345678**
7. **abc123**
8. **1234567**
9. **password1**
10. **12345**

The good news here is what constitutes being hacked can vary in severity. An account for a long-forgotten forum getting compromised is classified as a hack, but it's unlikely to have the same far-reaching consequences (unless you are reusing said password) as your bank account getting hacked.

However, at Bulletproof we often see these sorts of reveals as being a little misleading. These are all very poor, and very common passwords. However, the majority of apps or websites require an account of some description, seemingly regardless of how trivial they are. The sorts of accounts most likely to be compromised will belong to sites or services with poor security. It could be argued that when people make accounts for these, they are not too concerned about them and therefore, type the first password that comes to mind.



They are unlikely to take the same relaxed approach to their online banking or personal emails, not to mention most reputable websites have a strong password policy.

Such breaches though, are still useful in demonstrating that everything is a target. If it can be hacked, it will be. If anything, 2019 could well be when we finally started seeing the decline of the myth 'we're not important enough to worry about hackers'.

Hacking is occurring all the time. In fact, our honeypot demonstrated that a service exposed online can be discovered by potential hackers within 32ms. If a known vulnerability exists in this service, it can be compromised in hours or days at the most.

16 https://www.varonis.com/blog/likelihood-of-a-cyber-attack/

MY ORGANISATION ISN'T BIG ENOUGH TO BE A TARGET – THE MYTH EXPOSED

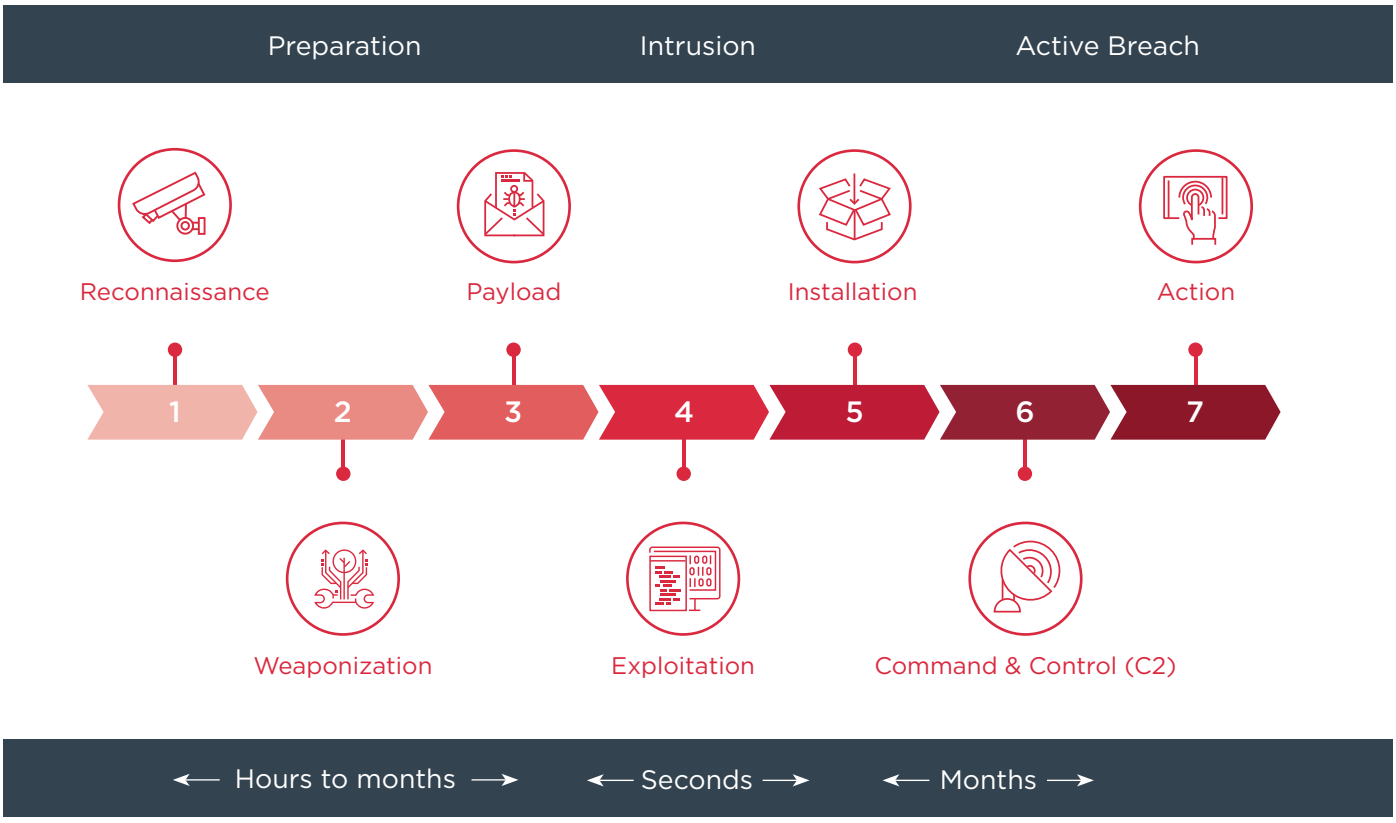
Sometimes, the mentality of a small business towards cyber security is one of the biggest problems. There seems to be a pervading idea that certain businesses or platforms aren't likely to be targeted because they're not big or interesting enough. This is entirely incorrect. No matter what size a company is or what they do, they are a target.

To prove this point, over the year we set up several honeypots. These consisted of isolated servers deliberately designed to include flaws of some description. We connected them to the Internet and waited. It is worth noting these servers were not connected to any business, big or small and nor did they contain anything particularly interesting.

One such server was left 'live' for a grand total of 2 days, 21 hours and 58 minutes. It was found (meaning contacted by external actors) within 32 milliseconds. This is likely to be from a bot which may or may not be malicious. However, it's still interesting to see that it takes less than a second for a service to be discovered.

To understand how this leads to a business getting hacked, it's worth mentioning the cyber kill chain. We've spoken a lot about the kill chain this year at events and on our website. It's the process that all hackers go through when compromising a business.

THE CYBER KILL CHAIN



The first step is reconnaissance. This is information gathering which, in this case, starts with scanning. The Internet is crawling with scanners continually identifying targets, which have their services and running components enumerated. Most importantly, scanners look for known flaws. This is happening 24 hours a day, 7 days a week. These scans are mostly conducted by automated bots, some of which are harmless, such as those scanning for indexing purposes. It should be noted, that the services running on our server would not have been of interest to such bots. As soon as any part of your business is exposed to the public Internet, it will be scanned. If there are any vulnerabilities found, they'll immediately become targets for further probing. It's often the case that scanners are looking for something specific, such as a piece of software with a known, exploitable vulnerability. It's after this you'll start experiencing signs of the next stages of the kill chain.

After being discovered in less than a second, we saw a slew of traffic. On average, we saw three malicious events per minute. In total, our server was contacted by 260 known bad actors, which are IP addresses belonging to people or organisations known to be malicious. We were contacted by 1,963 unique IP addresses and received a grand total of 12,757 requests.

All this focussing on one unassociated server with nothing of any worth on it. More to the point, it's worth noting that the exposed service was SMB, which is not typically exposed to the Internet and would not be something that's expected to be indexed. Which means, all IP addresses involved were likely malicious.

No matter how small, every company is a target.

If you pique the interest of a serious hacker, they'll switch IPs and begin their assault. They'll select a piece of malware, drop a malicious package, gain access to a database or even start making changes to the environment. Even our server would be of interest to certain malicious actors, in that it could be easily compromised and added to a botnet. It could then be used as part of a DDoS attack, which is still a viable threat to businesses. Whilst it seems they are dropping in regularity, DDoS attacks are growing in severity.

32ms found

3 unique contacts per minute

260 KBAs

1,963 unique IPs

12,757 requests received

CASE STUDY:

BAITING THE HACKERS WITH SSH

In another instance of our honeypots, we set up an SSH service. Once again this was immediately discovered and was hit with requests. The service stopped and started a few times (within the span of minutes) and throughout the day we saw multiple brute-force attempts.

Locations included:

- America
- China
- United Kingdom
- Brazil

In the span of half a day the service was contacted by 54 unique IPs, 40 of which were known to be malicious. 68% of the known malicious IP addresses were known for SSH brute forcing and the majority were from China and America.

Usernames attempted

- Pi – 4 times
- Root – 14,170 times
- Ubnt – 4 times

The huge number of attempts shows that this was indeed a targeted attack. SSH services are particularly appealing to hackers and they're able to try thousands of requests in short spans of time Anti-brute force mechanisms are easy enough to implement, but the fact that hackers continue to try it shows that a lot of businesses are failing to incorporate such controls into their network.

WHAT DO HACKERS GET OUT OF IT?

Even hackers won't necessarily know what they're going to get out of a hack until they've broken in and seen what's available. With our SSH example, we can assume there was very little effort required on their part. Arguably, the less effort required to hack a system, the more profitable it will be. There's always something to be gained as, even if there's no information to directly monetise, hackers will be able to add compromised systems to a botnet, which can then be rented out for a fee to commit DDoS attacks.

A hacker's primary motivation is monetary gain. 90% of hackers are motivated by financial gain or espionage. Of course, there are some that hack for political reasons or for fun, but they make up a much smaller percent.

Whilst state-sponsored attacks are rarer against businesses, on the whole the hackers will be better equipped. Nation states are likely to have technology and be aware of attack vectors that aren't available to the general public.

Nation states are likely to target third-party providers too, as attacking the supply chain is often a good way to access a target.

It's also true that the activity of nation states ultimately affects the general state of hacking. Attacks they develop often find their way into the public domain, meaning the lone hacker can make use of them.

HOW DO HACKERS MAKE THEIR MONEY?

Cyber criminals have many ways to monetise their misdeeds. Selling personal information on the dark web is one. With every breached database, more and more credentials, credit card details, passport information etc. appear for sale. Then there is ransomware. This method is still going strong with a rise in 2019 of 77% over the second half of 2018.

Cryptojacking, where hackers employ malware to syphon off CPU processing power to mine cryptocurrencies, was a hot topic in 2018. By the December of 2018 such attacks had risen by 450%. There hasn't seemed to be as much noise around cryptojacking this year, but that's not to say it's gone away. In the first half of 2019 there were 52.7 million registered attacks, and there are likely to be more the industry isn't aware of. The level of threat is directly linked to the value of the cryptocurrency being mined. The price of Bitcoin, for example, fluctuates wildly. When prices are high, mining tends to be high and vice versa.

Identity theft is a lucrative business for hackers. Stealing credit card information can be easy money if they can get to it. Card skimming malware (notably from MageCart) was a big offender last year. Then there's CFO/CEO fraud which makes use of sophisticated phishing techniques. Worryingly, 2019 saw the first instance of hackers using AI to impersonate a CEO to approve a payment, which is something we predicted at the end of 2018.

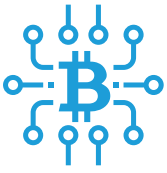
Blackmail was rife towards the end of 2018, with phishing emails making use of breached passwords to add an air of authenticity. Emails where hackers claimed to have compromised a user's system and have recorded embarrassing videos would demand payment in Bitcoin or they'll release the videos online. This was a rather short-lived campaign, most likely due to the press attention it received.

As mentioned, compromised assets can be added to a botnet which is then sold for DDoS attacks. These are admittedly on the downturn, but they are still a viable threat.

HACKERS MAKE THEIR MONEY THROUGH:

Selling personal information on the dark web

Ransomware



Cryptomining

SMES - ARE THEY BEING PRICED OUT OF THE MARKET?

With threats coming from everywhere in the world and targeting everything and anything, businesses need to invest in protective measures. As our honeypots show, no matter how small or uninteresting something is, it will be hacked.

It's concerning then that 51% of small businesses aren't allocating the right budget to cyber security. When you consider that 99% of UK businesses are considered SMEs[17] this is quite worrying. Even more so when you add the fact that in Q3 of 2019, cyber attacks against UK businesses were up 243%[18].

The cost of a data breach can reach the millions, which will often exceed the turnover of a smaller business. There are a lot of businesses relying on simple endpoint security products which just aren't up to the challenge of protecting a business. Even worse, as we have sometimes seen, companies aren't doing anything or doing very little to secure their systems. 74% of businesses don't believe they have the right personnel[19] (or do not have enough) to combat the cyber threat.

Many small businesses are finding adapting to GDPR compliance is also adding to the budget burden, meaning a lot of smaller companies are getting priced out of the cyber security market. Higher performing companies are allocating more budget to IT security, and as such, companies believe they have a stronger security posture as a result.

Getting the basics right needn't be that hard if you follow these 5 steps:

1. Know what is exposed (create an asset inventory)
2. Identify vulnerabilities (vulnerability scans and penetration tests)
3. Patch vulnerabilities and create a robust patching schedule
4. Provide staff with relevant training and test them
5. Enforce a strong password policy

74% of businesses feel they **lack cyber security personnel**.

Attacks against SMEs **increased** by **243%** in 2019.

SMEs are being **priced out** of the market.

17 https://labs.com/what-are-smes-why-are-they-so-important-for-the-uk-economy/
18 https://www.beaming.co.uk/cyber-reports/cyber-threat-report-q3-2019/
19 https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf

SECURITY IN HEALTHCARE

Having worked very closely with the NHS we've learned many important lessons this year that will help us improve security in this area going forward. One unavoidable issue is one of funding. There just isn't enough of it. Having a decent budget to fund cyber security projects is always beneficial.

That's not to say all problems can be solved simply by throwing money at it. A company can invest thousands into the latest tech, but if they don't know how to use it or what they need to be looking for, this won't achieve anything.

This leads nicely into another pressing issue in healthcare: people don't know what to look for. Unless your day-to-day job is security, you're unlikely to know what you need to be looking for in terms of threats. This is true for all industries, but healthcare is particularly complicated in that there's a lot of equipment being used, lots of outdated software and very little resources. As threats are always shifting, knowing what to look for is hard to explain to a general IT team. This is perhaps why this particular sector really stands to benefit from outsourced solutions.

Budget allocated to cyber security in healthcare is **1-2%** compared to the average **4-10%** of other sectors.[20]

Then there's patching. The healthcare industry: care homes, doctors' surgeries and hospitals etc. are among the worst offenders for outdated software. There are many contributing factors to this with budget restraints being among them. In some of our discussions in certain areas of this field, managers have freely admitted to not having a patching schedule in place. It's just too mammoth a task to consider for some.

In some instances, we have equipment hindering updates. Certain machines may not be compatible with more modern (and more secure) operating systems and taking them offline is simply not an option. The biggest challenge is we can't just take a hospital offline for a few days to update everything. An attack on this industry is worrying beyond the monetary cost. Disrupting services could cost lives.

It's interesting to think that hackers would take aim at healthcare services. If we consider the motivation of hackers to be primarily monetising their misdeeds, healthcare seems an odd target. Underfunded as it is, the industry is unlikely to pay ransom demands. The possibility of a disgruntled employee, script kiddie (someone who lacks expertise and makes use of known scripts) or even nation state cannot be discounted.

Why do they fall victim to attacks? Because they are incredibly likely to be caught up in an opportunistic attack. In the case of the 2017 WannaCry outbreak that crippled elements of the NHS, resulting in slowdowns and cancelled operations, it's likely they were simply collateral damage. They weren't targeted, but due to unpatched systems they got hit.

The silver lining of this incident is that the NHS came under more scrutiny and are currently working to improve things. Those we have spoken to within the industry have even stated that, without WannaCry, things might be a lot worse currently. Now the pressure is on and the NHS actively shares threat intelligence requiring action, but there is still the issue of time, as they are still struggling to make sense of this intelligence and prioritise actions.

20 https://www.thelancet.com/pdfs/journals/landig/PIIS2589-7500(19)30005-6.pdf

LOCAL AUTHORITIES GETTING TOUGHER

Local governments are often targeted by hackers for a variety of reasons, from the standard opportunistic attacker to politically motivated actors or even just someone looking to deface their site. Unfortunately, like many public sector industries, they're unlikely to have a huge budget for IT security.

We've seen a sharp rise in local governments contacting us for help with their security, from penetration testing, threat monitoring and even training. It's encouraging to see public authorities rising to the challenge of cyber security, and this may well have been influenced by the rise of GDPR and Cyber Essentials.

The challenge with local governments is not tied solely to budget. With lots of departments working on a range of different things and communicating with different people, the threats can vary from area to area. There's also a lot of sensitive personal information that will need protecting.

Ransomware can be particularly catastrophic to local governments and can bring services to a halt. If there's one thing we've learned this year overall, it's that ransomware doesn't look like it'll go away anytime soon. Though victims paying the demands are partly to blame. There's even been cases of businesses stating they can decrypt certain strains of ransomware. What they actually do is pay the ransom, before charging the victim more than what was originally demanded[21]. What's the easiest way to get ransomware onto a network? Email.

A large portion of the work we do for local government bodies involves cyber-security training.

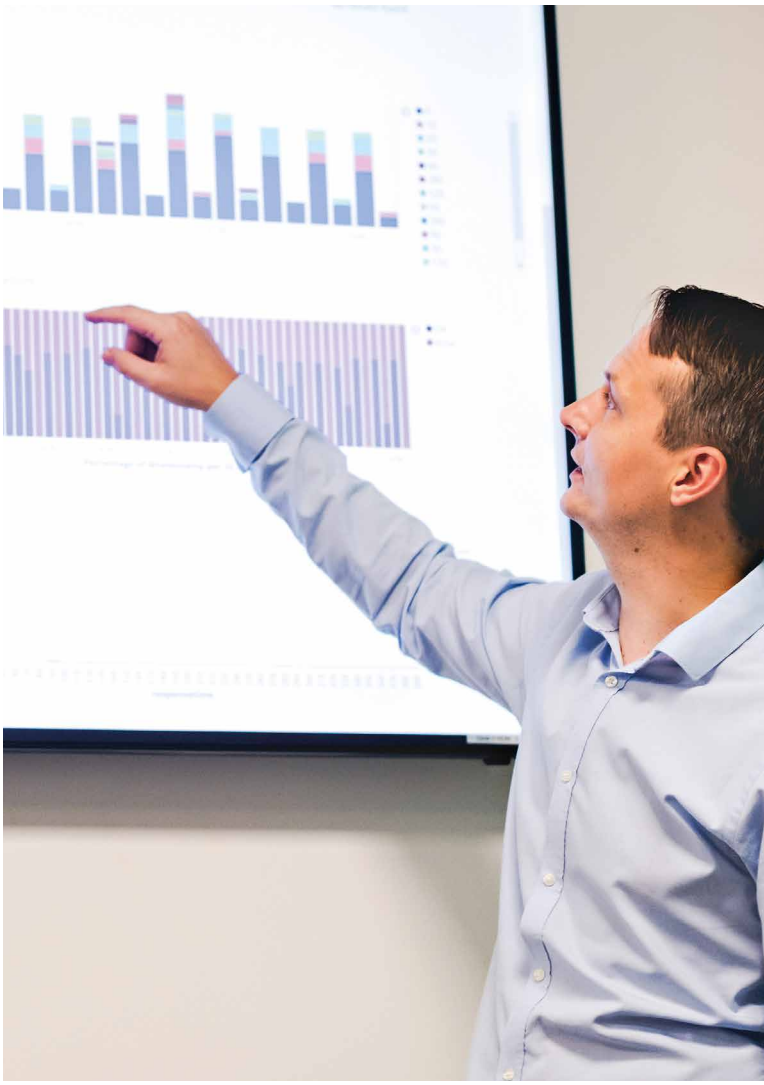
As we always say, you can have the best technology money can buy, but it can all be undone by an unwitting member of staff. Busy council offices and other public authorities are prime targets for the various forms of phishing. They're also good targets for a dropped USB stick. This, among other things, has proven that training is one of the most important aspects of a cyber security strategy.

Busy council offices and other public authorities are **prime targets** for the various forms of phishing.

PUBLIC BODIES INVESTING MORE?

From our own list of clients, we can see a trend of public services and authorities investing more in cyber security measures, including training, monitoring and penetration testing. From our own observations, awareness has grown significantly. Big, highly publicised attacks show organisations the damage a cyber attack can do and the cost they can have. Fortunately, these attacks often bring about change for the better.

It's an encouraging trend to see and we expect it to continue well into 2020 and beyond.



21 https://www.theregister.co.uk/2019/11/11/dharma_decryption_promises_data_recovery/

A YEAR WITH BULLETPROOF

The recurring theme throughout this report has been best practices. If companies can get the basics right, then the rest shall follow. Yet, the data clearly shows that organisations are struggling with this.

On the whole, the basic problems remain the same. Outdated software and components are still providing entrances to hackers, along with weak or default passwords.

The insider threat is as prevalent as always, either through accidents, negligence or malicious employees. Our honeypots seen in our research section have shown that hackers still follow the kill chain, meaning their approach hasn't really differed.

This seemingly lack of change is interesting though. We are all aware of the threats and breaches that are getting publicised all the time and yet, it would seem, organisations are still struggling to put up the most basic defences.

Pointing out a single reason for this would be difficult, as there are a lot of factors to consider. For a lot of companies, budget is a big one. Others are fearful that installing updates might stop something else from working as it should. They don't have the time or staff power to test everything in a staging environment first.

Start-ups and small to medium enterprises (SMEs) are more likely to be focussing their efforts and funds into expanding their business rather than into cyber security products. For others, security responsibilities fall onto the general IT team whose time is mostly taken up with the day-to-day technical affairs. For larger businesses, implementing best practices across a complex and sprawling estate may seem like too mammoth a task.

The fact is, implementing best practices across a business lays down the foundations to build a secure company. If businesses embrace security by design, maintaining security as they expand will be much easier.

The rise in interest in compliance packages is a step in the right direction. The majority of these, from Cyber Essentials to ISO 27001, work by instilling best practices at every stage, be it procedural or technical. The more companies look to gain compliance, the more likely we are to see positive change where cyber security is concerned.

If businesses embrace security by design, maintaining **security as they expand** will be much easier.

Of course, as businesses evolve, hackers look for new ways to compromise them. There's no telling what new threats 2020 will bring, but the harder an organisation makes it for hackers, the less likely they are to be targeted.

So, we hope 2020 will see more organisations get the basics right and incorporating privacy and security by design. Once best practices are maintained, the rest will follow.

BULLETPROOF

ABOUT BULLETPROOF

Bulletproof is a trusted provider of innovative cyber security products and people-centric services. We work with businesses of all sizes to protect their brand, value and assets against today's threat landscape.

Organisations rely on our managed security services to protect, detect and respond to cyber threats at any time of the day. Our dynamic portfolio of services include next-generation cyber protection via our S.W.A.T. Defence® managed SIEM, 24/7 SOC, CREST certified penetration testing, as well as a wide range of compliance and cyber security solutions tailored to the exact requirements of our clients.

For further information on Bulletproof's services and how we empower great results for our customers visit: **www.bulletproof.co.uk**

bulletproof.co.uk

01438 532 900

contact@bulletproof.co.uk

PCI DSS COMPLIANT
PCI DSS v3.2
Level 1 provider

24/7
24/7 on-site Security
Operations Centre

CREST
CREST approved

THE BRITISH ASSESSMENT BUREAU
ISO27001
ISO 27001 and
9001 certified

TIGERSCHEME
Tigerscheme
qualified testers

SC SMART THINKING. DELIVERED.

Part of the ServerChoice Group.
Learn more at ServerChoice.com