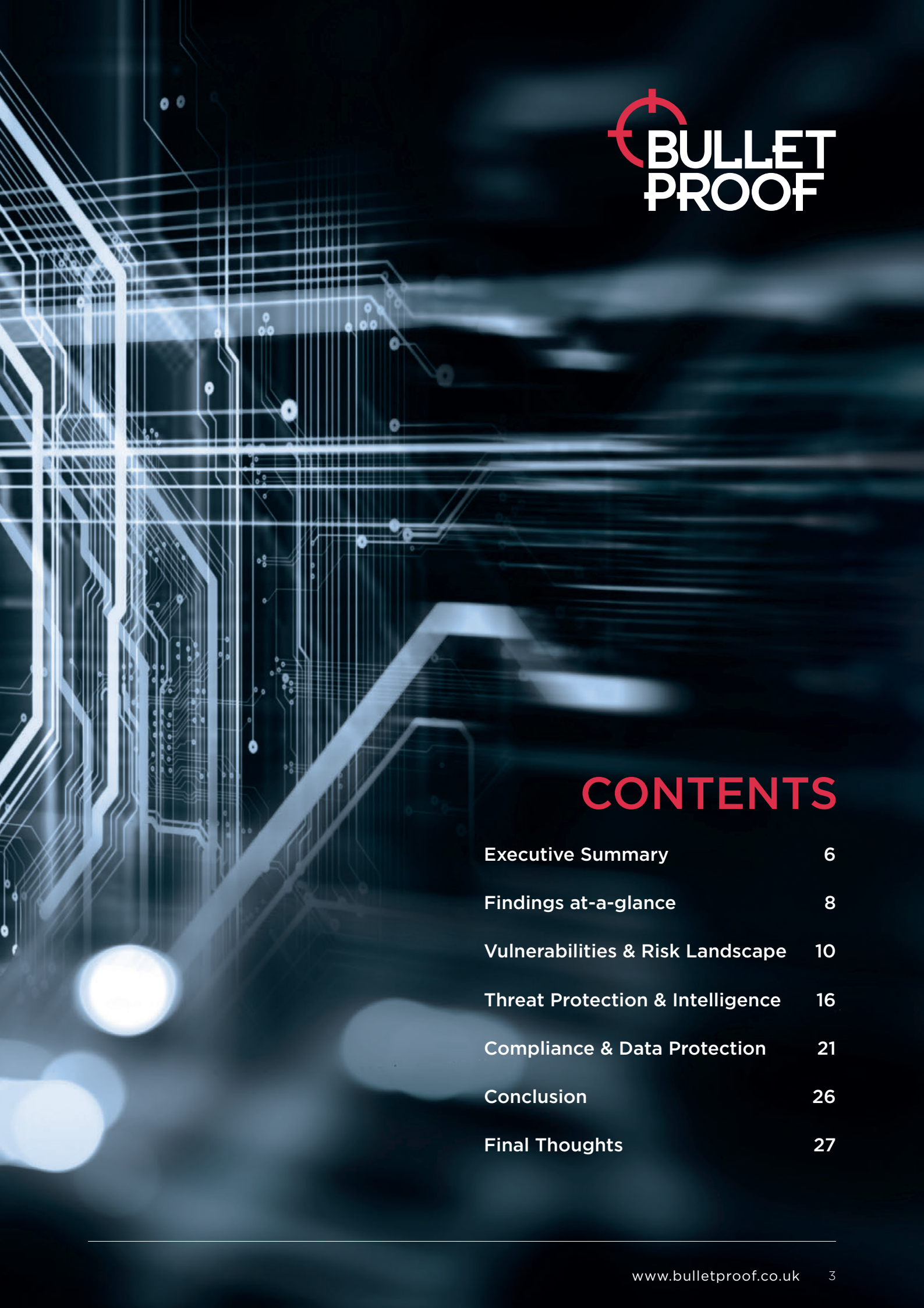

BULLET
PROOF
BULLETPROOF
ANNUAL
CYBER SECURITY
INDUSTRY REPORT
2021
www.bulletproof.co.uk

Bulletproof is a trusted provider of innovative cyber security products and people-centric services.

We help simplify and solve the cyber security challenges for organisations across all industry sectors to protect their brand, value and assets against today's evolving threat landscape. Organisations of all sizes rely on our security services to protect, detect and respond to cyber threats.

Bulletproof's dynamic portfolio of services includes CREST-certified penetration testing, proactive threat monitoring services, 24/7 SOC, compliance support, security training and much more.



CONTENTS

THOUGHTS FROM OUR CEO

THOUGHTS FROM OUR CEO

The changes brought about by the global challenges in 2020 were truly unprecedented and represent a real shock to the system for businesses of all sizes and industries.

As with every year, I was surprised that so much has changed in the security landscape, but that so little is different in business attitudes. Despite the enormous upheaval in technology, people and processes, the way organisations secure themselves largely has not changed. For many this results in greatly weakened defences, and it's possible that we haven't yet seen the biggest exposure of a large remote workforce.

Oliver Pinson-Roxburgh
CEO & Co-Founder

The changes brought about by the global challenges in 2020 were truly unprecedented and represent a real shock to the system for most businesses, playing into the hands of hackers. This will no doubt lead to unexpected threats in the future and responses will be need to be revisited. Disruption always leads to new opportunities for hackers, and the necessity in 2020 to adopt new technologies, build new processes and support a new way of operating has caused great risk. Security implications were sometimes left unconsidered as the initial focus for businesses was on getting back online, not implementing a secure system for future remote working. This year our data proves that remote working will introduce significant risks to businesses and their employees.

On to the report itself, and I was excited to again see such interesting data. Throughout my career I have often been frustrated that although we see a huge amount of evolution in both cyber attacks and cyber defences, the basic attacks are still the most successful for the hacker. This is more prevalent in SMEs than in mid-market organisations, but across all business sizes we see that businesses struggle to truly embed security, resulting in similar issues across all vertical markets. Businesses are innovating faster every year to get a commercial competitive edge, and this in itself causes problems: how do you secure what you don't fully understand? To compound this problem, many of the most innovative solutions do not yet provide a feature-complete set of controls that would allow you to protect it. Security and compliance need to be seen as an enabler rather than a disabler of innovation and company growth, and this attitude should also come from the top down, starting with the board. The data really does show that you need to be on top of your testing and proactive monitoring. Even those that are investing in security assessments and security services have flaws in their pen tests and are under attack. The thought of significant cyber security investment does not stop an attacker or mean that you automatically get more secure applications and infrastructure.

The typical mantra of a hacker is "if it ain't broke don't fix it", and our data shows that this remains true for opportunistic hackers. However, this year we have seen an interesting transition in the hackers' approach. From statements being made that hacking groups would not be targeting healthcare services during the pandemic, to some groups reviewing financial records to see if companies can afford to pay them during a ransomware attack, it's certainly an interesting time to be a cyber security vendor.

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

This report highlights interesting outcomes on data taken from our industry research, staff experience, penetration testing, SOC, honeypots, compliance, and data protection activities. Bulletproof explores all these areas and more as we look back through 2020 to learn what we should keep in mind for 2021 and beyond.

It will come as little surprise to anyone reading this report that cyber security activities in 2020 were dominated by the Covid-19 outbreak. This caused organisations of all sizes to make a swift transition to mass remote working to ensure business continuity. What would typically take months of planning was implemented in a matter of days. The disorder that this created, combined with the already uncertain nature of life during a pandemic, produced the ideal environment for cyber criminals. This scramble to the 'new normal' created interesting vulnerabilities, that were both detected in our penetration testing exercises and protected against by our SOC. Despite the dominance of Covid-19, there was plenty in the field of security and privacy that was not related to the global pandemic, and it's these findings that often make for the most interesting reading.

KEY INSIGHTS

Based on our penetration testing data and industry research, we've analysed the vulnerability and risk landscape of 2020 and made several discoveries. One notable finding was the drop in prevalence of outdated components as the top critical vulnerability identified during a penetration test. Whereas this flaw accounted for over 50% of all critical flaws in 2018 and 2019, it dropped in 2020 to only 32%. This is owing to the increased adoption of cloud infrastructure and SaaS services, and corroborates our other findings such as an 80% drop in NBNS attacks (which typically don't work in cloud environments) compared to last year.

> Another significant finding was the 350% increase in phishing websites and the rise in coronavirus-related phishing emails.

Phishing was already a large attack vector for an organisation, and when considered with our finding that only 3% of penetration tests included social engineering, it paints a perilous picture of organisations not taking this increased risk seriously.

Our SIEM and SOC data fed into our threat protection and intelligence section, revealing that simple best practices are still not being followed by businesses. 85% of all brute-force attacks involved just three sets of default credentials. Hackers continue to try these credentials in this attack type for one reason: they continue to work. Our intelligence activities revealed that only 1.7% of malicious IP addresses we detected were in commercial threat intelligence feeds, proving that trusted relationships with managed security service partners is more valuable than ever.

> When it comes to compliance and data protection, Covid-19 has had a large part to play in 2020.

Rushed remote working implementations had an impact on virtually all security compliance standards, as well as the GDPR. Many companies were in breach of standards and regulations without even realising it. This increased the challenge for compliance auditors as well as Data Protection Officers (DPOs), who were already burdened by the uncertainty of Brexit on data privacy matters. Throughout 2020, Supervisory Authority/ Regulatory activity was light compared to European standards, with the UK's ICO handing out only four fines under the GDPR.

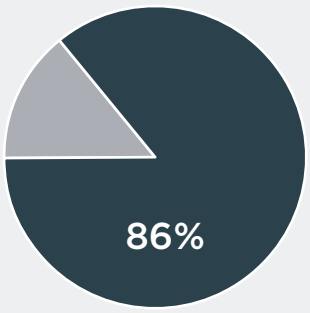
CONCLUSION

Upon analysing the data and uncovering the stories it tells, it was revealed that SMEs and mid-market companies are facing separate problems, though both have also had to contend with hackers pivoting their attacks to take advantage of the unprecedented global situation. We undertake a full exploration of the specific challenges each organisation size is facing in the conclusion at the end of this report.

FINDINGS AT A GLANCE

ATTACKS ARE INCREASING ON UK BUSINESSES[1,2]

MICRO SMALL MEDIUM LARGE



86% of UK organisations expect attacks to increase significantly in 2021

WHO ADMITS TO A BREACH?

IMPACT OF BREACHES ON UK BUSINESSES[1]

33%
Report losing customers after a data breach

11%
Didn't know whether they had been attacked

"What these stats show is that every size of organisation is at-risk of a cyber attack. The real concern is how many breaches go un-reported or even un-noticed. Low capability to detect an attack will always influence breach statistics.

HOW COMMON ARE CRITICAL, HIGH AND MEDIUM ISSUES?

1 in 4 critical
1 in 4 tests revealed a critical flaw
In 2019 and 2018 it was 1 in 5

1 in 2 high
1 in 2 tests revealed at least a high flaw

3 in 4 medium
3 in every 4 tests revealed at least a medium flaw

TOP 3 CRITICAL WEAKNESSESS

32%
Outdated & vulnerable components

9%
SQL injection

8%
Broken access control

"This shows that the number of critical flaws is increasing, meaning that organisations need to take their cyber risks extremely seriously or face the potentially ruinous consequences.

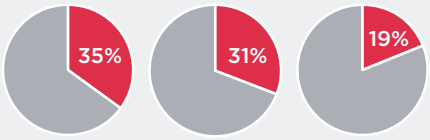
FINDINGS AT A GLANCE

CAN YOU RELY ON COMMERCIAL THREAT INTELLIGENCE?

OVER 9,000

IP addresses we identified as belonging to bad actors, only 158 (1.7%) were in the top commercial and open-source threat intelligence feeds.

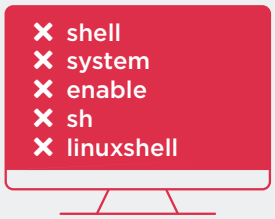
DEFAULT CREDENTIALS ARE A SIGNIFICANT VULNERABILITY



= 85%

85% of honeypot attacks were made up of 3 username/password combinations: Admin/admin **35%** Root/admin **31%** Admin/password **19%**

MOST COMMON COMMANDS RUN ON HACKED MACHINES



> Commercial and open-source threat intel is a good source of data but can't be relied upon on its own. The continued prevalence of brute-forcing default credentials is down to one thing: it continues to be a successful attack method for cyber criminals.

TOP 3 GDPR FAILURES

INTERNATIONAL VS UK GDPR FINES[3]

Spain 50+

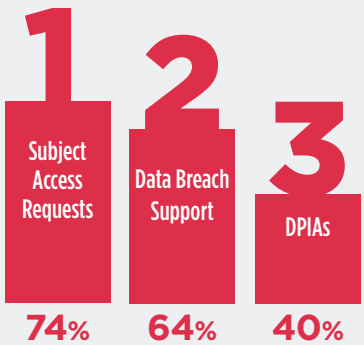
Italy 20+

Belgium 20+

UK only issued **4 GDPR fines!**

November 2019 to November 2020

TOP 3 DPO ACTIVITIES



> The high percentage of companies failing GDPR compliance on Individuals Rights correlated with our high DPO activity of assisting with Subject Access Requests. 2020 has been a slow year for regulatory action from the ICO, made worse as a result of Covid-19.

VULNERABILITIES & RISK LANDSCAPE

VULNERABILITIES & RISK LANDSCAPE

FOREWORD

Kieran Roberts
Head of Penetration Testing

"Largely it's been 'business as usual' during 2020 for the penetration testing team, even taking into account the Covid-19 outbreak. We were already in the process of rolling out new technology to facilitate remote internal infrastructure testing when the lockdown happened. This meant we were well prepared to continue providing all penetration testing services. Another, less positive, element of business-as-usual trend was the continued prevalence of critical security vulnerabilities due to outdated components. Organisations take risk-based decisions, and for many the greater risk was responding to employee remote working, rather than patching legacy infrastructure.

Bulletproof's testing activities actually increased year-on-year, as organisations realised the security implications of the sudden shift to remote working. The findings of this year's report accordingly show an uptick in cloud adoption that solves some security problems, but also creates new challenges. Whatever the situation, Bulletproof stands ready to deliver."

STATS SUMMARY

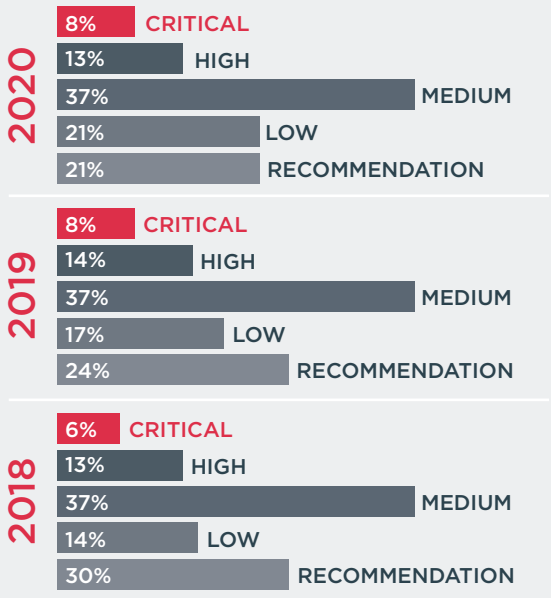
HOW COMMON ARE CRITICAL, HIGH AND MEDIUM ISSUES?

1 in 4 critical
1 in 4 tests revealed a critical flaw. In 2019 and 2018 it was 1 in 5

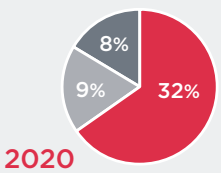
1 in 2 high
1 in 2 tests revealed at least a high flaw

3 in 4 medium
3 in every 4 tests revealed at least a medium flaw

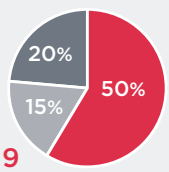
HOW SEVERE ARE THE DISCOVERED FLAWS?



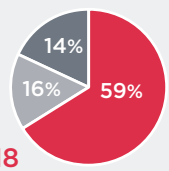
TOP 3 CRITICAL WEAKNESSESS



2020
- Outdated & vulnerable components
- SQL injection
- Broken access control

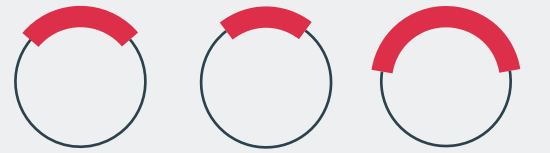


2019
- Outdated & vulnerable components
- Broken access control
- Weak cryptography



2018
- Outdated & vulnerable components
- Cross-site scripting
- Weak cryptography

MOST COMMON TEST TYPES



28% Application only

21% Infrastructure only

45% Application & infrastructure

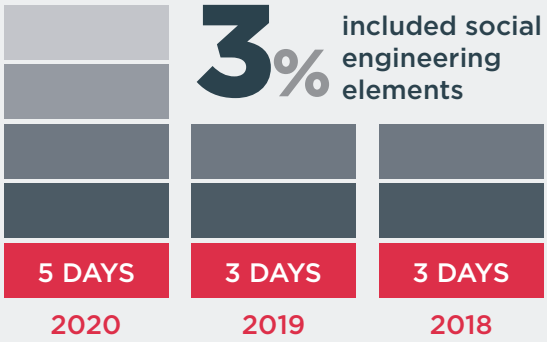
MOST COMMON CRITICAL ISSUES BY SECTOR

Internet & Technology
Weak cryptography

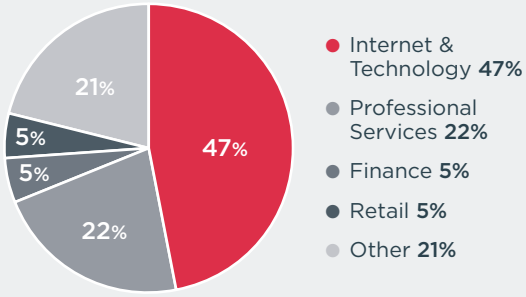
Professional Services
Broken access control

Finance
Out-of-date & vulnerable components

AVERAGE LENGTH OF PEN TESTS



WHO'S SPENDING THE MOST ON PENETRATION TESTING?



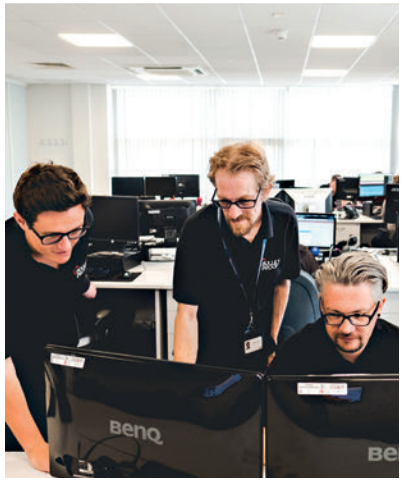
CHANGING LANDSCAPE

The most significant change seen in the penetration testing landscape was the rapid shift to remote working and the 'new normal' that emerged after the first few weeks of the UK Government's coronavirus response. Such a mass change in working practices affected the way cyber criminals operate, the way people respond to attacks, and how cyber security vendors like Bulletproof delivered services.

Hackers will always act quickly to turn any situation to their advantage, which was reflected in a 350% rise in phishing attacks in Q1 alone[4]. Using the coronavirus outbreak in the phishing content played on people's fear and desire for information about the pandemic, resulting in higher engagement levels and, ultimately, more successful hacks. The rise in phishing success was mirrored in Bulletproof's phishing campaigns, though we avoided any coronavirus-themed messaging so as to not upset anyone who might have been legitimately affected. We found that with people working from home our phishing campaigns were drastically more effective. This is primarily down to a lack of interaction: staff can no longer quickly lean over and ask their colleague what they think of a suspect email. Add to this a lack of procedural and technical security oversight, and it's easy to see how phishing represents a high security threat to a business.

Whilst phishing, which was already a significant attack vector, increased in severity, other methods employed by hackers decreased. In last year's report we highlighted the prevalence of NBNS attacks, however this year our findings show that NBNS attacks dropped significantly and quickly, down by over 80% by May 2020. The reason for this is a technical one: NBNS attacks do not work as well over a VPN. Given the rise in VPN adoption as a result of staff working from home, hackers acted quickly and dropped this previously successful attack vector.

NBNS attacks dropped significantly and quickly, down by over 80% by May 2020.



CLOUD FOCUS

Our testing showed that the trend towards the cloud is continuing, with increasing numbers of environments being 100% cloud-based, typically AWS and Azure.

Notably, internal networks are now being migrated to the cloud, as is end-user software, thanks to the rise of software-defined networks and Office 365 ubiquity, respectively. This presents fresh challenges for penetration testing and new limitations on what can and cannot be tested. For example, it's typically not possible to get a dump of passwords from cloud services, meaning penetration testers can no longer brute-force passwords offline to test their effectiveness and use them as part of their testing activities.

The inability to bulk-acquire passwords is one of many security benefits that increased cloud adoption provides, but the challenge for organisations is in making the most of the opportunities. Migrating to cloud services presents the prospect to re-work a business' IT estate to build-in security at a fundamental level. This is an easier task for SMEs than for mid-market companies, however SMEs generally aren't aware of security implications and thus don't take advantage. As such, when testing we typically find that many implementations of both SMEs and mid-market cloud migrations are rushed and, as a result, introduce even more security vulnerabilities.

Similarly, the cloud could help with the number one critical-rated vulnerability we find during testing: that of unpatched and outdated components. This is reflected in this year's stats, where outdated components represented only 32% of critical vulnerabilities, down from over 50% in the previous two years. This figure would be lower still if it were not for the grey area of shared responsibility, where organisations either aren't sure, or don't know, who's responsible for what between them and their provider. Mid-market organisations with their larger infrastructures have the additional problem of being too sprawling to be effectively managed by overworked IT teams, meaning systems get forgotten about and so go unpatched. In a world where an unpatched Adobe product is just as critical as unpatched Windows OS, this makes for varied penetration tests and long remediation lists.

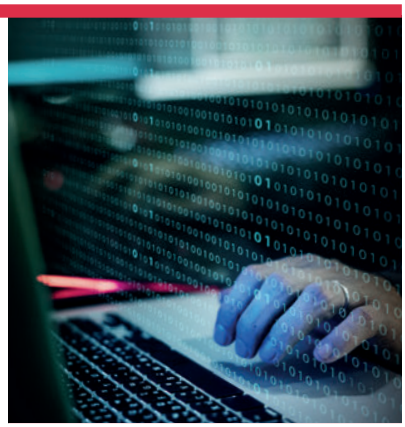
Overall, our testing shows that cloud adoption is making business infrastructure generally less complex, though few businesses are making the most of the opportunity to increase their security. The move to the cloud conversely makes penetration testing activities more complex with various locations and technologies to contend with, such as containerisation, shared responsibility models, on-premises, hybrid and public cloud deployments.

Outdated components represented only 32% of critical vulnerabilities, down from over 50% in the previous two years.

WEB HOMOGENISATION

Bulletproof's penetration testing activities have uncovered an increasing trend of homogenisation in underlying web technologies, which presents often-overlooked risks to a business. The risks of web homogenisation have been quietly building for a number of years, notably 2014 and the Heartbleed vulnerability which affected OpenSSL, a security system. However other technologies, which aren't directly security products, are now reaching the point where they become a security risk thanks to their market saturation.

A popular example is WordPress, which as of 2020 powers 38%[5] of all sites across the web and is particularly popular with SMEs. Out-of-date WordPress installations and its plugins are common vulnerabilities uncovered during testing, meaning a new security vulnerability discovered potentially impacts thousands of businesses. Similarly, CloudFlare, which is used by approximately 15%[6] of the entire web (over 12 million domains), had an outage on 17th July 2020, affecting many businesses[7]. An Azure Active directory outage in September crippled many web services, reportedly including 911 services in the US[8]. The lesson here is to carefully analyse the third parties you rely on, based on your risk appetite. New technology, such as Bulletproof's Recon Scan, can highlight the reliance on third-party providers to help organisations take a risk-based approach.



Carefully analyse the third parties you rely on based on your risk appetite.

KEY TAKEAWAYS

VULNERABILITIES & RISK LANDSCAPE

- Organisations aren't investing in social engineering, with only 3% of tests including phishing. Internal campaigns remain challenging for businesses to conduct successfully as it relies on thinking like a hacker. This results in businesses leaving their biggest cyber risk untreated.
- The proportion of discovered severities remain broadly similar to the past three years – a trend we expect to continue.
- There are fewer critical vulnerabilities discovered per individual test, but more tests have at least 1 critical flaw. This shows the level of security is normalising, driven by cloud adoption, web homogenisation and increased certification of compliance standards.
- Out-of-date components has reduced its lead as the number one cause of critical severity, again thanks to increased cloud adoption as well as compliance standards such as Cyber Essentials.
- Companies across all industries are procuring longer tests. This realisation of the value of penetration testing is partly driven by increased supply chain compliance.
- The internet & technology sector spends the most on penetration testing, which aligns to their innately higher risk level given the nature of their business.
- Increased working from home has led to a rise in phishing, with a 350% increase in phishing websites in Q1 alone[4].
- Organisations are moving from infrastructure testing to app testing and combined infrastructure and app testing. This reflects the larger move towards the cloud and websites being delivered as apps.
- The increase in cloud and containerisation technology adoption can help increase security, but these opportunities aren't taken, leading to new attack vectors.
- The shared responsibility model of cloud service providers leads to grey areas and security oversights that often go unnoticed, introducing so-called stealth risks.
- Web technology homogenisation is reaching a tipping point where it should now be considered as part of your security strategy.


THREAT
PROTECTION &
INTELLIGENCE

THREAT PROTECTION & INTELLIGENCE

FOREWORD

Andy Smith
SOC Team Leader

"Despite the turbulence of the past year, one constant has been the need for good security. Monitoring plays an integral part of this, being a source of continuous stability amidst the security flux. At Bulletproof we stood ready to respond to hackers' new attack vectors as the world changed. With approximately half of our managed SIEM clients radically changing the way they worked, we had to change with them and re-learn customer environments and create new security baselines and runbooks.

The data from our honeypot provides interesting reading, proving that attackers are still seeing users as the weak point within an organisation, attacking passwords and attempting to brute force their way into accounts. This is also validated by data identifying the significant rise in phishing attacks, which has been a focus area for our proactive monitoring team. The data shows that everyone with an internet presence is being continuously tested by hackers, and that phishing can bypass the security of businesses who've invested in technical security controls, but not procedural/human ones."

STATS SUMMARY

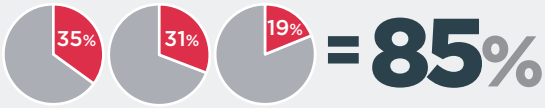
HONEYPOT DATA

OVER 9,000

IP addresses we identified as belonging to bad actors, only 158 (1.7%) were in the top commercial and open-source threat intelligence feeds.

Over 12 million

failed logon attempts within 5 months

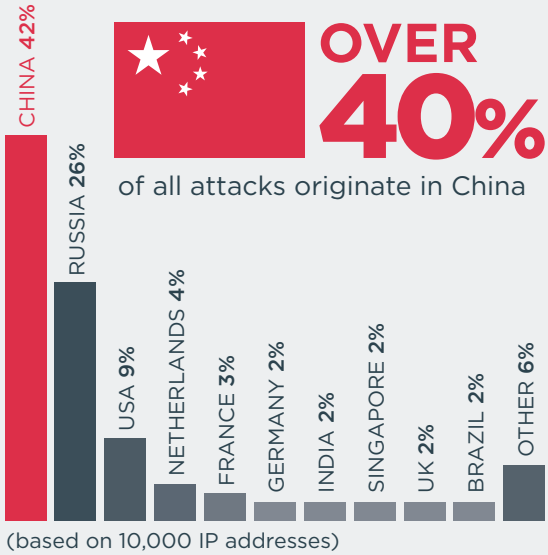


85% of honeypot attacks were made up of three username/password combinations:
Admin/admin **35%** Root/admin **31%**
Admin/password **19%**

TOP FIVE

Most common commands run on hacked machines

- shell
- system
- enable
- sh
- linuxshell



OVER 40%

of all attacks originate in China

(based on 10,000 IP addresses)

BULLETPROOF SIEM DATA

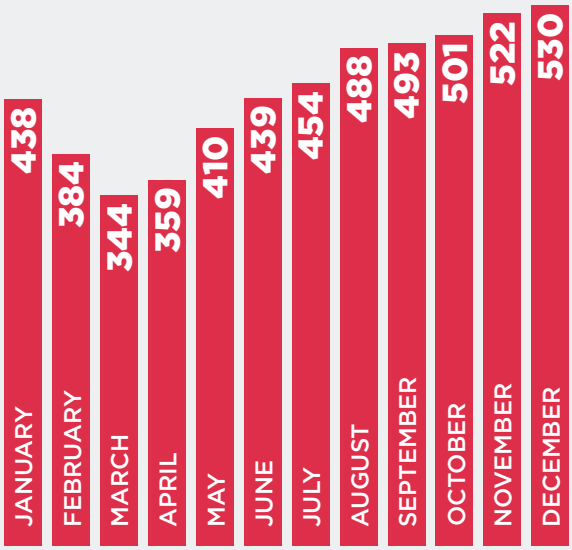
1,000,000,000

Over 1 billion logs ingested by our SIEM every day

OVER400

Analyst-investigated events raised per month

Security events raised per month during 2020



HONEYPOT FINDINGS

Bulletproof's SOC team set up several honeypots across different public cloud environments, in order to bait hackers and catch them in the process of hacking. This is an extremely valuable source of primary intelligence which complements commercial threat intelligence sources and feeds directly into the SIEM platform that powers the Bulletproof MDR service, S.W.A.T. Defence®. Our honeypots show the attack tools and techniques that cyber criminals are using in the wild in real-time, making it an effective front-line resource in our efforts to proactively prevent attacks to client infrastructures.

HACKERS CUSTOMISE ATTACKS

Our data has shown that even opportunistic cyber criminals chasing a quick win will conduct recon on the machine they're attempting to compromise. For example, upon changing the name of a machine in our honeypot network to 'HR Workstation', we saw attackers adapt their brute-force username attempts from 'administrator' to 'sage' and 'sage server'. This creates the opportunity for novel modes of cyber defence in the form of obfuscated, or even deliberately misdirected, machine names as part of a deep defence strategy.

All security advice, from loose best-practice guidelines to rigid certification standards, recommend or mandate changing default login credentials. As our honeypots have shown, that's for good reason. Even with changed passwords, easily guessable usernames such as 'administrator' or 'root' still provide a lock for a cyber criminal to try to pick. This security challenge is exacerbated by the use of cloud services, as login panels are often accessible from any geographic location. For SMEs, the challenge is in gaining awareness of this issue, which can be solved by standards such as Cyber Essentials. For mid-market organisations, the problem is in maintaining secure configuration across a vast and changing IT estate. Again, compliance standards can help here by baking-in best practices across the business.

GLOBAL DISTRIBUTION

Our research this year reveals that China-originated attacks have dropped from 55% to 42%, and Russia has risen from 6% to 26%. This year's statistics are in-line with what security industry researchers would expect to see and shows maturation from last year's intelligence. The inclusion of China and Russia as the top two countries for bad actors continues the trend of past years, though it should be noted that geographic location can be spoofed, and that hackers often don't care about international borders thanks to the ease of being anonymous. The relatively high proportion of attacks coming from the USA (at 9%) is likely because the new Bulletproof honeypot network makes use of a variety of public cloud environments in multiple territories, including the USA. This made our honeypots more visible to US-based hackers and is more reflective of the threats businesses face.

REFLECTED ATTACKS

Data from our honeypot shows that, compared to last year, hackers are increasingly using compromised machines for reflected attacks. This is where the hacker's goal isn't the data on the machine itself, but rather to use the compromised machine as part of a larger attack against a third party. This helps a hacker reduce their chance of detection and reduce the chance that an attack will be linked back to them. Over 50% of reflected attacks were non-secure HTTP (port 80) attacks on ya.ru, a Russian email and search provider. The next 3 of the top 5 targets were all secure HTTPS (port 443) attacks on YouTube, Google, and Instagram. Last place in the top 5 attacks was SMTP (port 25) attacks against Yahoo!. This evidence confirms that the SME mindset of 'I'm too small to be a target' is false: if you're easy to hack, you're a target.

SIEM SERVICE FINDINGS

CHANGING EXPECTATIONS

2020 saw a marked increase in the number of organisations who look to their security partner to provide an end-to-end service, from detection to action. For example, let's say Bulletproof has detected unauthorised scanning activity from an IP address that our threat intel determines is malicious. Rather than escalating this to an organisation's security or sysadmin team with a recommendation to block the IP, organisations are looking for their security partner to automatically block the offending IP. This has both advantages and challenges, which need to be carefully analysed on a per-client basis, using various factors including their internal resource, risk appetite, and business type. Proactive action is a powerful security defence and forms a core element of S.W.A.T. Defence®, however we would always recommend that businesses have contacts within their organisation who can respond to security events. This is where good processes in pre-defined runbooks – a staple of any effective MDR service – comes into its own.

COVID-19 IMPACT

During February to May, the number of security events raised by our SOC team dropped by over 10%. Our service delivery was unaffected by Covid-19, as our SOC team and systems remained working at full capacity throughout the year, so the explanation for a temporary drop in security events must lie externally. Analysing our extensive SIEM data reveals that the drop in security events was driven by two factors: change freezes and a shift away from VPN to cloud services.

Change freezes are where a business elects to not make changes to their infrastructure, such as a software upgrade or commissioning a new server, and are often implemented over Christmas due to lower staff availability. The Covid-19 situation caused similar issues of lower staff resource and the degraded capability to respond meant organisations, most typically mid-market, swiftly implemented change freezes.

The rush to implement remote working brought about by Covid-19 led to a swift migration to cloud productivity services, such as Office 365. This often bypassed the use of a corporate VPN, which was a data source for the SIEM, not to mention a prime security control. As soon as a client informed us of their migration to a cloud service, our SOC teams worked hard to swiftly connect it to our SIEM platform so we could maintain oversight of their security. In contrast to the change freezes, this was mostly driven by the SME sector more than mid-market.

Notably the drop in events starts in February, before the March lockdown, as businesses acted swiftly in an attempt to get ahead of the developing situation. This shows a proactive approach to security and business continuity which is in-line with expectations of a business who has invested in a SIEM service such as Bulletproof's S.W.A.T. Defence®.

KEY TAKEAWAYS

THREAT PROTECTION & INTELLIGENCE

- China and Russia remain the top territories for bad actors, continuing the trend of previous years.
- Commercial threat intelligence is a valuable resource, but can't be relied upon on its own, making a business relationship with a trusted security partner even more vital.
- Hackers recon the type of machine they're trying to attack and customise their attacks accordingly, offering new opportunities for defence mechanisms.
- Brute-forcing default credentials is a common attack because it continues to work, showing that basic security defences commonly aren't implemented.
- Hosting in the cloud enables more brute-force attacks as hackers no longer need local access to your environments, further highlighting the importance of basic security controls.
- Covid-19 remote working caused a temporary drop in security events as mid-market organisations implemented change freezes and SMEs pivoted to cloud services.
- Smaller organisations are increasingly leaning on security partners to provide an end-to-end service, from detection to action (such as blocking IPs), thanks to a lack of internal resource.
- Reflected attacks are increasing, with big global brands (Google, Instagram, Yahoo etc) as the top targets. This shows that your business can be a target not because of any intrinsic value in your services or data, but just because your security is breachable.


COMPLIANCE
& DATA
PROTECTION

COMPLIANCE & DATA PROTECTION

FOREWORD

Nicky Whiting
Head of Compliance

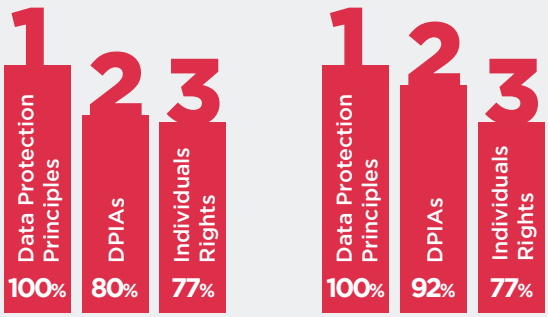
"It's been another challenging year in the world of compliance, particularly given that Covid-19 has thrown up many privacy and security scenarios organisations didn't previously have on their radar. A key point I've noticed this year is the push for security and privacy in the supply chain. Some organisations are going overboard with supplier due diligence by making large demands of smaller companies, which is out of proportion to the risks these smaller companies present to their businesses. During the course of next year, I predict we'll see a shift from this overly cautious attitude to a more graded and sensible approach.

The Schrems II (Privacy Shield) ruling is set to have a big impact on a lot of UK business. Like everyone else, we await further guidance from the ICO and EDPB, but the outcome will only increase the compliance burden on DPOs and privacy officers.

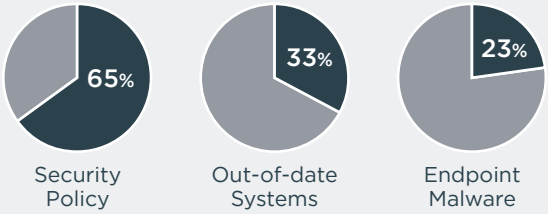
One thing is for certain: nothing stands still in the world of compliance, which in some ways presents a challenge, but in others it's what makes it interesting and makes those of us who work in this industry get out of bed every morning."

STATS SUMMARY

TOP 3 GDPR FAILURES



TOP 3 AREAS OF CYBER ESSENTIAL FAILURES



TOP 3 DPO ACTIVITIES

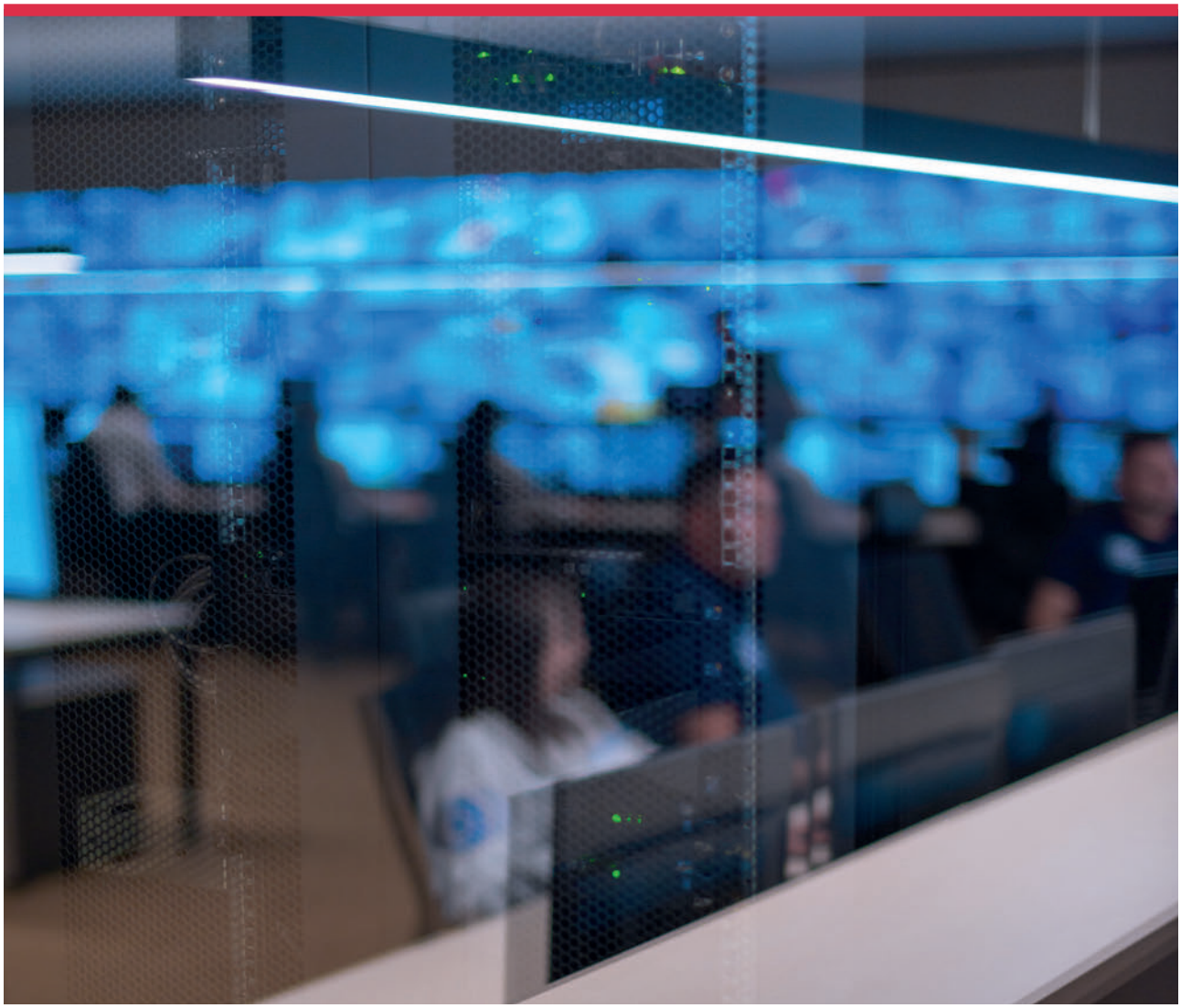
TOP ICO FINES

British Airways were fined **£20,000,000** under GDPR[9]

INTERNATIONAL VS UK GDPR FINES[3]

November 2019 to November 2020

CYBER ESSENTIALS



2020 saw the release of a new Cyber Essentials framework that, on the surface at least, doesn't appear to be notably different. It still covers the same 5 technical controls and it's still managed via a simple questionnaire. The one significant change is that the certificate now needs to be renewed every year, which should encourage organisations to maintain good standards of security.

Additionally, the base level of Cyber Essentials became quicker to achieve as it no longer requires a vulnerability scan. This has slightly encouraged adoption and made first-time passes easier, as there's less work required to achieve compliance. When companies do fail, it's typically on security policies, out-of-date systems, and a lack of endpoint protection – all of which are basic measures.

The one significant change is that the certificate now needs to be renewed every year, which should encourage organisations to maintain good standards of security.

GDPR

The coronavirus outbreak and associated response by both Government and businesses caused many organisations to unwittingly breach GDPR compliance. The test, track and trace method meant people regularly left their personal data in every restaurant they visited, without any consideration by a lot of hospitality businesses of the need to protect this personal data in-line with the GDPR. The Department of Heath also admitted that the Test and Trace system was implemented without a data protection impact assessment (DPIA)[10]. The impact of Covid-19 also slowed down the ICO's GDPR investigations – a process that was already criticised for being too long.

Bulletproof's data showed that the most common GDPR failures have stayed static since 2019, which illustrates that it's the core tenets of the GDPR that businesses are failing to grasp. Our research did reveal one notable increase in failures this year which is down to a lack of enacting and/or recording GDPR refresher training. Regular training embeds the GDPR as a culture within a business, and is vital to its effective implementation. Without it, GDPR awareness levels will drop and mistakes start to be made — leading to higher risk of data breaches. Bulleproof provides data protection services to a wide range of verticals and organisation sizes and our research has revealed that the most common areas our DPOs get involved in are largely unchanging despite these differing circumstances:

SUBJECT ACCESS REQUESTS (SAR)

This can be a time-consuming process for organisations who aren't prepared for it, and many businesses aren't fully aware of their obligations when it comes to actioning a SAR.

DATA BREACHES

Data breaches are an intimidating proposition without expert help on hand. Our DPOs help organisations determine if a breach needs to be reported, what data is affected, and the process to follow.

DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

DPIAs are a fundamental component of the GDPR and many organisations need a helping hand to confirm when one is required, and to verify they're following a suitable procedure.

Regular training embeds the GDPR as a culture within a business

ISO 27001

2020 saw ISO 27001 increasing in take-up thanks to an enhanced awareness of supply chain risks. Many companies have realised that their suppliers are their weakest link, plus there's encouragement from an increased overall awareness of risk and dependency supplied by the GDPR. The initial momentum was with larger organisations, but it rapidly flowed down the chain to smaller organisations also. However, this has been hampered by the Covid-19 response and the challenge of remote working. Not only has it introduced new scope for a variety of non-conformances, but it has also added new challenges to the process of auditing.

Covid-aside, the challenges ISO 27001 compliance faces remain unchanging since last year: the standard is not maintained as BAU and not embedded as culture, with many businesses still seeing it as a tick-box exercise. Significantly, this is a top-down problem: without leadership buy-in, ISO 27001 compliance is extremely difficult to maintain. IT/Procurement teams may be driving the requirement, but without senior management on-board the project it will always be an uphill struggle.

BREXIT UNCERTAINTY

Brexit continues to be a source of concern and confusion for everyone in the compliance industry, with no details known or suspected before they're announced by the Government. This makes for a challenging time for those people responsible for data protection within an organisation. The Schrems II ruling that effectively struck down the Privacy Shield arrangement further complicates matters, though learnings from the outcome here can help inform the UK's strategic position.

KEY TAKEAWAYS

COMPLIANCE & DATA PROTECTION

- Cyber Essentials has become quicker to achieve and is required for Government, MoD and NHS contracts, further increasing its universal appeal and applicability.
- GDPR failures haven't changed since 2019, showing that it's the core principles that are being misunderstood.
- Organisations are benefitting from support from their DPO in these three main areas regardless of industry or size: SARs, data breaches and DPIAs.
- The Schrems II ruling shook up the privacy community at a time when it was already trying to cope with the uncertainty around Brexit. The striking down of Privacy Shield has increased the due diligence burden on businesses and requires a more vigilant approach.
- An uptick in ISO 27001 compliance is being driven by increased supply chain awareness, which can disproportionately burden SMEs.
- Compliance implementation broadly faces the same challenges as with previous years: that of lack of leadership buy-in for the project resulting in it not being embedded as a culture within the business.

CONCLUSION

The statistics and findings presented in this report paint an interesting picture of the dynamic state of cyber security in 2020. However there's one last story to be told. Upon analysing the data and listening to the real-world experience of our teams, we have discovered that the challenges faced by businesses are more common to the size of organisation than which vertical industry they operate in. Accordingly, this conclusion will address the challenges faced by both the SME and mid-market sectors.

VULNERABILITIES & RISK LANDSCAPE

The prevailing attitude of many SMEs is unfortunately one of ignorance, specifically in thinking that their size does not make them a target, despite statistics routinely showing otherwise. 68% of medium-size businesses reported attacks in the last 12 months, and given that many cyber attacks go unnoticed for months or even years, we can safely assume this percentage to be even higher. The bright side of the SME situation is that their problems, when discovered, are typically easier to fix than their larger counterparts thanks to a greater operational agility and less mature infrastructure.

Mid-market companies have the opposite problem: cyber security spending is high on the agenda and regular testing is typically part of business-as-usual. However, the penetration tests themselves are more demanding and when problems are found, they can be difficult to remediate in a timely manner. With complex infrastructures spanning multiple environments, third-party providers, legacy systems and shared responsibility cloud services, much co-ordination is required to fix even the simplest security vulnerability.

THREAT PROTECTION & INTELLIGENCE

SMEs increasingly demand their security protection to provide them with full uptime protection against cyber attacks, but at the same time lack the internal resources to deal with incidents as they arise. Leaning more on their security partner to backfill this gap can be a useful compromise in situations where low resources and lack of board buy-in put higher internal security spending out of reach. SMEs typically have the flexibility to pivot to cloud services with greater ease than mid-market companies, but lack the expertise to ensue they do so securely.

Mid-market organisations meanwhile have a tougher time migrating to the cloud as they lack flexibility, but are generally better prepared to configure securely – assuming they invest the resources up-front to do so. Our monitoring has revealed that mid-market organisations' struggle is in maintaining secure configuration in a sprawling and changing infrastructure.

COMPLIANCE & DATA PROTECTION

The challenges facing SMEs are primarily a lack of internal knowledge and staff resource. This is particularly apparent in the 40% rise in outsourced DPO services being delivered to SMEs. In general, staff within SMEs cross-resource, meaning there's little scope for an internal SME DPO to operate without a conflict of interest. The SME space can also be something of a wild west when it comes to security and privacy controls: the most elemental of controls, such as access control or password management, may simply not exist. Security fundamentals such as regular security training and Cyber Essentials certification can go a long way to solving this. Cyber Essentials also forms a good basis for pivoting to GDPR and ISO compliance in due course.

Conversely, mid-market organisations typically have established security and privacy controls, and generally good processes. This makes achieving certification a relatively simple process, however the challenge for mid-market organisation comes in the form of maintenance. Their more mature infrastructure and complex business organisation make maintenance activities proportionally more demanding in time, resource, and expertise. Whilst a GDPR DPIA or data flow map for an SME might be straight-forward, for a mid-market company it can be a significant challenge. The struggle of compliance maintenance builds up as time goes on, resulting in a frantic (and expensive) scramble when it comes to an audit. By spreading compliance maintenance throughout the course of the year, mid-market businesses can drastically ease the process, however this is reliant on making compliance a true part of business-as-usual culture.

FINAL THOUGHTS

Oliver Pinson-Roxburgh
CEO

A lot has changed in a short period of time and business leaders need to be wary of the impact and risks this represents. Being proactive and monitoring for threats can help secure your future, but you also need to secure your past. Review what has been done to get the business back on track and ensure corners have not been cut that could expose the company, its employees and customers to cyber criminals.

Now that large proportions of businesses staff are remote working, it's even more important to be a good custodian of data. Many organisations are now operating wholly outside the walls of security investment made by their company, as security has been put into the hands of staff that are not security professionals and often do not have a good grasp of risk. In addition, hackers are using open-source and off-the-shelf security tools to reduce the chances of being detected, as custom tools often lead to easier attribution for security researchers.

Cloud has been catapulted into the forefront of many business strategies, and despite the assumption is that it is inherently secure, the truth is that it's only as secure as you configure it to be. I have seen businesses that have sadly already paid the price of moving too fast.

Security and compliance are business enablers that all businesses should embrace, aspiring to get true value from compliance, not just check a box. Many compliance standards are now already being mandated as part of a procurement process and thus a mature approach will put you ahead of your competitors.

SOURCES

This report is based almost exclusively on original research using anonymised data from Bulletproof's cyber security, compliance & data protection services, as well as our staff's valuable experience of managing and delivering the services.

Where our research as been supplemented by external data sources, these have been noted with in-text citations. The corresponding sources are listed below:

1 https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020

2 https://www.realwire.com/releases/Survey-reveals-86-of-UK-businesses-expect-cyber-attacks-to-increase

3 https://ico.org.uk/action-weve-taken/enforcement/

4 https://www.itpro.co.uk/security/phishing/356704/un-report-points-to-a-350-rise-in-phishing-website-at-start-of-2020

5 https://en-gb.wordpress.org/download/

6 https://w3techs.com/technologies/details/cn-cloudflare

7 https://blog.cloudflare.com/cloudflare-outage-on-july-17-2020/

8 https://www.theregister.com/2020/09/29/onedrive_azure_active_directory_outage/

9 https://ico.org.uk/action-weve-taken/enforcement/british-airways/

10 https://www.wired.co.uk/article/nhs-test-and-trace-unlawful-data

BULLET PROOF

www.bulletproof.co.uk

01438 500 500

contact@bulletproof.co.uk