Emerging Trends 2021

Exploring the changing cybersecurity landscape

Inspiring trust for a more resilient world

Contents

"The world has seen an increase in cyber-attacks relating to COVID-19, reemphasizing just how vital information resilience is for organizations."

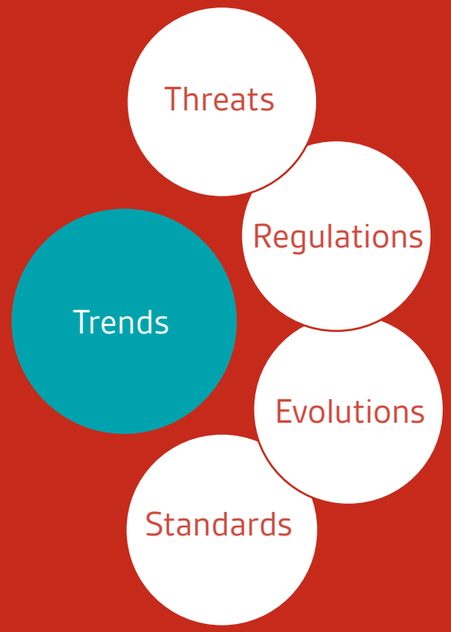
Mike Bailey

Director – Consulting Services (Cybersecurity and Information Resilience)

Introduction

With the turbulent year that was 2020 drawing to a close, we look to the future and hope for a brighter 2021 for us all. 2020 has been a year that has seen so much change, evolution and forced innovation, you may be forgiven to hope for a period of extended stability moving into the new year.

Over the course of 2020, the world observed wholesale transformation. This influenced the way in which we live our daily lives, our working styles and the way our national health organizations operate. However, one of the more surprising changes came about in just how responsive organizations can be in the face of unprecedented situations.

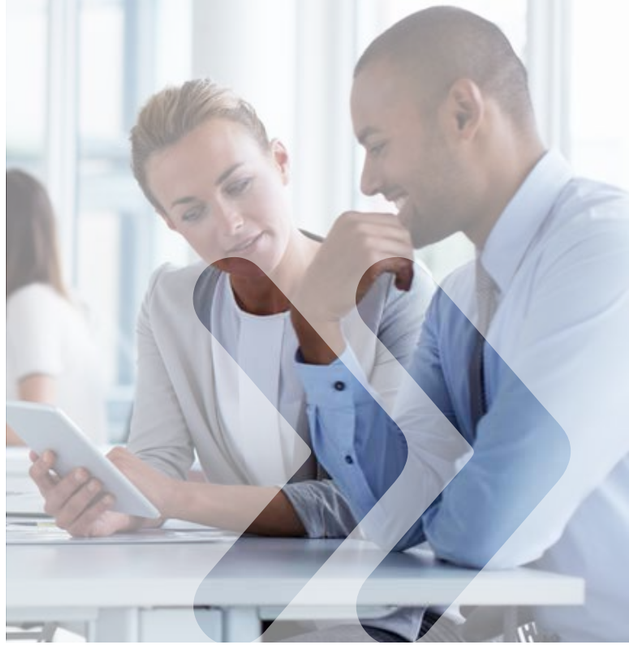


BSI's consultants observed even the most risk averse and slow to move organizations react at breakneck speed to take swift decisions and either retain, relax or toughen security policies and practices in order to keep the lights on.

In many cases, the choice made was dependent on the maturity of IT capabilities and security functions. In cases where this worked well, many senior leaders asked, 'Why can't our IT functions move at this pace all the time?' For others, questions were asked as to why changes resulted in negative impacts to the organizations.

A key risk evident in many businesses related to the inability to access systems, leading to insecure remote access and authentication practices, resulting in increased successful attacks or malware incidents.

While every organization will recognize that they received and, in many cases, blocked at least some form of attack relating to COVID-19, some organizations felt the pain more acutely. Regardless, the three mainstays of the cybercriminal remain atop the 2020 list – Phishing, Ransomware and Privacy regulations. Based on this, it is prudent to expect that where the attack model works for cybercriminals, we can expect re-investment into attack advancement and defence bypass to further exploit those willing to pay ransoms in 2021. These attacks put a spotlight on how vital information



resilience is for organizations. Value is always subjective, and it can rapidly change depending on the circumstances in which a company finds itself.

There are also other significant trends on the horizon for 2021, including further changes to regulations, standards, and attacks, as well as strategies on how to handle these changes effectively. In this paper BSI will provide insights into specific areas of focus across determined regulations and standards, as well as emerging evolutions and threats, demonstrating that vaccines will not be the only game changer in 2021.

Data protection and privacy management

Navigating turbulent seas

Mary Kennedy

Consultant – Cyber, Risk and Advisory

Matt Cooper

Director – Cyber, Risk & Advisory

While companies are still trying to understand and comply with significant changes in global privacy regulations in 2020, they should anticipate another year of rapid change in the global regulatory environment.

Rounding the corner on 2020, a year that many are happy to put behind them, we look to the new year with a fresh sense of hope and optimism. However, for those of us responsible for setting the strategic direction of global privacy compliance, many challenges remain. In fact, things may get even more hectic than they were in 2020. The main issues that are likely to drive the privacy agenda include Brexit, Schrems II and continuing legislative evolution on both a national and global level.

The turn of the year sees the completion of Brexit, and a pre-determined assessment of adequacy by the EU for the UK is not forthcoming. This inevitably impacts the free flow of personal data between the two jurisdictions. In any case, Brexit means organizations should adopt a risk-based approach and identify business critical transfers of personal data to and from the UK/EU. Additionally, organizations will need to assess whether they fall under the scope of Article 27, GDPR and appoint an EU or UK Representative to meet that requirement (which is in place under both the EU and UK's data protection regimes).

Looming large over the privacy landscape is the 2020 "Schrems II" decision by the Court of Justice of the European Union (CJEU), which invalidated the EU-U.S. Privacy Shield as a lawful mechanism for transferring data to the US. The CJEU, however, did leave the door open a crack to the possibility of lawful transfers by confirming the validity of Standard Contractual Clauses ("SCCs") as long as additional safeguards are included to protect data protection rights to EU standards. Subsequent interpretations by the European Data Protection Board (EDPB), and some of its constituent

5,000

Almost 5000 organizations relied on the EU/US Privacy Shield, struck down by the CJEU in the "Schrems II case"*

"2021 will continue to see high impact data protection issues dominate the compliance landscape, and organizations need to be alert to the continuing evolution of their compliance challenges."

References

www.europarl.europa.eu/RegData/etudes/ATAG 2020/652073/EPRS_ATA(2020)652073_EN.pdf

www.dataprotection.ie/en/news-media/latest-news

ico.org.uk/action-weve-taken/enforcement

*www.privacyshield.gov/list

Regulators have all but slammed that door shut. Their subsequent interpretation and guidance suggests that, unless “supplementary measures” prevent processing of personal data in clear text by US companies, it is all but impossible to demonstrate that those companies can provide “essentially equivalent” privacy guarantees to those provided by the GDPR.

In addition to these EU focused challenges, an upswing in California Consumer Privacy Act (CCPA) lawsuits, the passage of the California Privacy Rights Act (CPRA) as well as a broad range of US State-level and international changes to privacy regulations (e.g. New Zealand, Canada, India, Brazil) will keep data privacy and legal teams scrambling to stay on top of their organizational compliance and risk management.

Individuals are the ultimate beneficiaries from increased data protection rights and privacy protections. Whereas companies and organizations collecting and processing personal data are at greater risk of loss than ever before from regulatory actions and legal or civil suits.

BSI’s privacy practice has been helping global organizations to adapt to the ever-changing landscape and thrive in the pursuit of innovative, business enabling compliance practices. BSI’s expert privacy team assists our clients to leverage

external privacy requirements to innovate new solutions and technological approaches, help minimize compliance risk, adopt privacy best practices and future-proof their business.

BSI’s Cybersecurity and Information Resilience (CSIR) consultancy is enabling businesses and organizations to successfully navigate the turbulent waters of privacy management in 2021.

“BSI has been helping global organizations adapt and thrive, leveraging external privacy requirements to innovate new solutions and technologies.“

References

*edpb.europa.eu/sites/edpb/files/consultation/edpbrecommendations_202001_supplementarymeasurestransferstools_en.pdf

curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf

InfoSec 2021

Third-party assurance is now required

Matt Cooper

Director – Cyber, Risk & Advisory

Third-party security certifications and attestations like ISO 27001 and SOC 2 used to be a competitive advantage, they are becoming a necessity.

We work with your team every step of the way, from "just getting started" to ongoing compliance monitoring with any information security or data privacy certification scheme including ISO 27001/27018/27701, SOC 2, CMMC, FedRAMP, proprietary attestations related to MS SSPA, or regulations like the NYDFS CRR, GDPR, or HIPAA.

There was a time when forward-looking organizations, and those in "sensitive" or "high-risk" verticals, allocated precious resources towards an ISO 27001 certification or SOC 2 Type II attestation report in order to differentiate themselves from the competition in the area of information security, stand out from the crowd, and provide their customers with greater assurance that their products and services would not increase their customer's risk of a data breach or some other loss event. Things have changed.

As we move into 2021, several different market trends are aligning to the point where the cost of security certification, for many organizations, is going to be less than the cost of "doing nothing."

Take for instance the US Department of Defense (DoD) decision to require the roughly 300,000 contractors in its supply chain ecosystem to certify to the appropriate level of the Cybersecurity Maturity Model Certification (CMMC) scheme. The DoD decision demonstrates what many in the industry already know, which is that while an organization may insert a "right to audit" clause in a supplier contract, such audits are rarely performed due to the time and expense for the auditing company, not to mention the auditee. Without an actual audit, the DoD and industry professionals understand that a company's self-attestation of their own controls in response to a security questionnaire is of limited value. Again, the cost to truly investigate and assess those third-party responses is significant and executing that type of third-party validation process at scale is prohibitively expensive and time consuming for most organizations.

Complementing this trend is the emergence of compliance and audit automation platforms, which are particularly effective for smaller, cloud-native service providers. Setting aside the question of their reliability, almost every technical scanning product now provides the option to report on the "ISO 27001 compliance" or "HIPAA compliance" of their systems and networks. In addition, products are emerging which combine an "audit management portal" with reporting dashboards aligned to the security or reporting framework of your choice (e.g. SOC 2, HIPAA, PCI etc.) and provide control-aligned evidence repositories. These platforms, in theory, simplify the work effort for the auditor, provide more consistent outputs and, perhaps most meaningfully, can significantly reduce the cost of the third-party audit for the auditee.

In this new landscape of commoditized compliance audits paired with hard security assurance requirements from government and enterprise class customers, the cost of "doing nothing," which includes completion of lengthy security questionnaires and the manual effort of explaining your security posture to every prospect, is greater than the cost of certification.

"As we move into 2021, several different market trends are aligning to the point where the cost of security certification, for many organizations, is going to be less than the cost of "doing nothing".

References

www.dfs.ny.gov/industry_guidance/cybersecurity

gdpr.eu

www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html

www.bsigroup.com/en-US/our-services/cybersecurity-information-resilience/services/iso-27001-consultancy

oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf

PCI DSS v4.0

Watch this space

John Hetherton

Global Practice Lead – PCI DSS

PCI DSS v4.0 is due to be released mid-2021. The new standard allows an outcome-based approach, as well as the usual prescriptive control set, introducing more flexibility to the previously uncompromising standard.

27.9%

Only 27.9% of organizations meet compliance at the first pass*

PCI DSS is known for its prescriptive control set and validation processes. It has often been criticized (and sometimes lauded) for its rigidity compared to some of the more risk-based security standards. As such you can expect to see the following areas of focus in PCI DSS V4.0:

- Added flexibility and support methodologies to achieve security outcomes;
- Security as a continuous process
- Enhanced validation methods and procedures, including new future dated controls.

This additional flexibility will allow adaptability for organizations to achieve security outcomes, which is particularly useful in environments which are evolving rapidly, for example cloud.

Some control areas which have attracted particular attention in the Request for Comment feedback include:

- Authentication, specifically consideration for the NIST MFA/password guidance
- Broader applicability for encrypting cardholder data on trusted networks
- Monitoring requirements to consider technology advancement

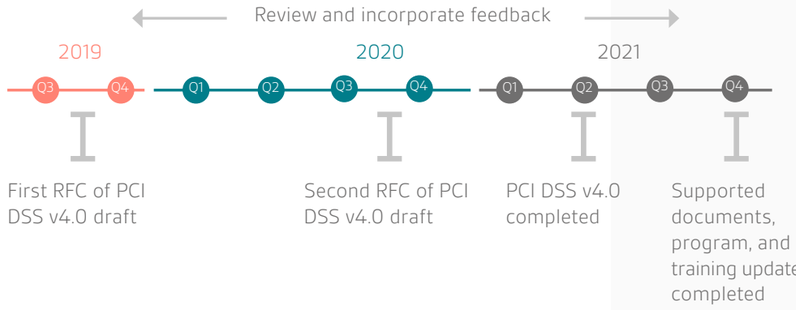
It is likely you will see some changes in these areas as well as in others, as the standard attempts to keep up with the evolving technology and threat landscapes.

PCI DSS v4.0 is due to be published mid – 2021. PCI DSS v4.0 and Version 3.2.1 will run in parallel for 18 months, giving organizations time to migrate across to the new standard.

Achieving and maintaining PCI DSS compliance will not be made simpler under PCI DSS v4.0, however more flexibility will be introduced as to how you achieve and maintain that compliance.

Continuous monitoring of control efficacy and integration of compliance tasks into BAU will remain key to ensuring high levels of continuous compliance, a firm requirement if an organization is to maintain as secure cardholder data environment and leverage safe harbour in the event of a breach.

"Achieving and maintaining PCI DSS compliance will not be made simpler under PCI DSS v4.0, however more flexibility will be introduced as to how you achieve and maintain compliance"



References

www.pcisecuritystandards.org

*www.verizon.com/business/resources/reports/payment-security-report

From siloed to collective protection

A cybersecurity shift

Herman Errico

Practice Manager EMEA
Cyber, Risk & Advisory

In the current business landscape – where the acceleration of digital transformation has been the norm – aligning business, cloud and security strategies has become increasingly important. Therefore, a shift from siloed to collective protection is necessary to navigate uncertainty and succeed as a business of the future.

73%
of "leading" organizations view a strong security team as a contributor to business success*

Traditionally, a siloed protection approach has focused on protecting business assets with limited inputs or alignments to overall business objectives. A modernized collective protection approach focuses on protecting assets, while achieving mutually agreed business results. Results that are fully achievable if security teams and business stakeholders work together and understand their priorities.

Security teams have always focused their efforts in implementing security controls to protect business critical assets. Such efforts were led by multiple drivers, including regulatory compliance, internal policies or third-party requirements. When implemented well, this has been effective to protect these assets. However, this methodology has not always developed solutions to empower the business, and in some cases were misaligned with business objectives.

This assumption is in line with the idea of a centralized security model that most security teams follow. A centralized security team focuses on identifying the security risks and determining the mitigating controls in line with industry best practice. However, the main pitfall lies in the design and implementation of a security control, which is often performed by security personnel without taking into account potentially valuable inputs from the wider business.

By shifting towards an agile approach and embedding security and privacy champions that collaborate with wider business stakeholders, more in depth and productive business conversations become natural. As such, rethinking the security governance structure of a security team from simply a support function to a 'value add' function will be required to successfully navigate future market uncertainty.

In 2021, we foresee an increase in such initiatives amongst many security teams and a shift from being a siloed function to a business enabling partner. BSI helps organizations and their security teams to redesign their security strategies and to shift from siloed to collective teams.

"In 2021, we foresee security teams shifting from a support function to a business enabling partner within the organization."

References

*www.thesslstore.com/blog/cyber-security-statistics/#cyber-security-statistics-what-organizations-are-investing-in-cyber-security

Trust in 5G networks

Isabel Forkin

Head of Cyber Lab Services

5G is the next generation of mobile communications, bringing us many benefits including faster connectivity and latency. As organizations plan their use of 5G, security must be integrated from the start.

1/3 of the globe
By 2025, 5G* networks are likely to cover one-third of the world's population*

The 5G network is the next revolution in mobile computing. It provides faster speeds, less lag and higher capacity than previous generations, and it will enable a more resilient decentralized network of distributed devices. The potential use cases are endless, from supporting AI to delivering automated infrastructure and beyond.

5G uses virtualization technology to deliver dynamic networking capabilities, called software-defined networking (SDN). To ensure successful integration within an organization, the addition of new 5G enabled technologies must consider security requirements throughout the lifecycle. This can be achieved by including security in the design and architecture, completing ongoing risk assessments and a robust testing programme.

For many organizations, the primary advantage of 5G is that the communication paths and networks become de-centralized, where computing power moves to the 'edge' (e.g. closer to sensors or end users). This presents interesting challenges around securing the 'edge', and how to protect data and processes that are physically and logically removed from centrally managed security controls.

One possible option is to implement the 'Zero Trust' model, where devices on the network are not assumed to be safe, and security perimeter controls are replaced with confidence in each individual connection made. In this model, devices are not inherently trusted just because they are the 'right' side of the perimeter. This changes how the security perimeter is defined and helps to fully utilize the advantages of 5G.

As organizations start to use ths advance in technology, they must plan how it will be used securely. Organizations need to understand what risks this introduces into their environment and how this affects their information, networks and systems. When security is included by design, organizations can have confidence in the security of distributed 5G networks, and the data they carry and process.

"To ensure successful integration within an organization, the addition of new 5G enabled technologies must have security designed and built in from the beginning."

References

www.ncsc.gov.uk/blog-post/zero-trust-architecture-design-principles

*www.ncsc.gov.uk/information/5g-explainer

www.ncsc.gov.uk/blog-post/blog-post-security-complexity-and-huawei-protecting-uks-telecoms-networks

www.ncsc.gov.uk/whitepaper/security-architecture-anti-patterns

Intuitive security for users

Beyond training and awareness

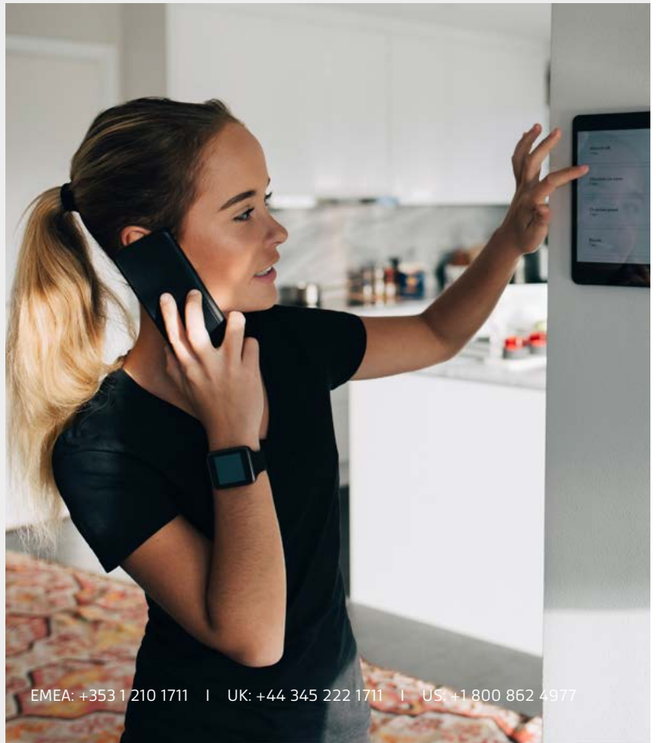
Isabel Forkin

Head of Cyber Lab Services

Product designers are responsible for helping users make secure choices, and systems should be secure 'out of the box'. Security testing should include in-depth understanding of default configurations and how users will secure a device in-life.

When we think of how humans affect security, we often think in terms of what they might do wrong; social engineering, accidental compromise, etc. We usually mitigate this with training or, if a company has a mature security programme, a technological solution like Data Loss Prevention (DLP).

The human in front of the keyboard is often considered the weakest link, but one thing we sometimes ignore is how systems are designed to help users make secure choices.



This is becoming a more frequently asked question in security. For example, the number one control in the the UK's Department for Digital, Culture, Media and Sport (DCMS) code of practice for IoT is 'No default passwords'. This helps prevent one of the most common attacks against IoT systems, without relying on the user to be security-conscious. As computing becomes more distributed, this will be increasingly important.

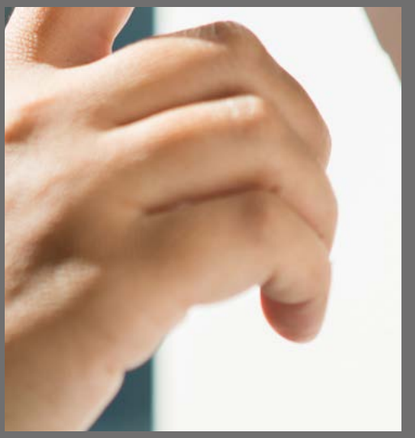
This shift toward providing a secure device 'out of the box' is important for home consumables, but it is also important for corporate systems. We often forget that administrators are human too.

We sometimes see misconfigurations as a failing of the device administration, or a result of the tension between security and functionality. But administrators shouldn't have to disable Telnet or change default password. As technology diverges it becomes more important that systems support administrators provide a secure configuration by default.

To support this, the National Cyber Security Centre in the UK has set up a sociotechnical team who look at the questions of how users interact with systems and identify where there are cracks in the security introduced through insecure user designs.

As product certification evolves, we are seeing a higher emphasis on testing 'default' configurations and developing an understanding of how systems support secure choices. To be ahead of the curve, manufacturers need to include these important questions in their security testing scope.

"One thing that we often ignore is how systems are designed to help users make secure choices."



26 billion

There are more than 26.66 billion IoT devices active in 2020*

References

www.ncsc.gov.uk/information/secure-default

www.ncsc.gov.uk/blog-post/a-sociotechnical-approach-to-cyber-security

www.gov.uk/government/publications/secure-by-default-self-certification-of-video-surveillance-systems

*www.ncsc.gov.uk/static-assets/documents/stg_infographic_july.pdf

Secure Access Service Edge (SASE)

Cloud-delivered defence in depth

Michael Green

Senior Cloud Security Consultant – Security Technologies

Three major trends that we have seen and will continue to see through 2021 are the continued shift to remote working, expedited cloud migrations, and the associated targeted attacks on these developments.

72%

of organizations plan to assess or implement Zero Trust capabilities in some capacity to mitigate growing cyber risk*

The workforce at large is now connecting to enterprise applications and accessing information from remote locations outside of traditional corporate networks. Previously, organizations may have routed internet-bound traffic back via the security stack in their datacentre, but this is expensive, wasteful, and less valid as applications move to the cloud, whilst limiting scalability and sustainability. In addition, backhauling traffic and client virtual private networks (VPNs) can result in a less secure and bad user experience. Being tasked with and accountable for consistently protecting workforces and data regardless of location or device is a big challenge.

Thankfully, there are cloud-hosted solutions that enable organizations to protect assets, preserve the user experience, and add value that was not possible with locally hosted security offerings due to architectural limitations – one of which is the Secure Service Access Edge (SASE) model. SASE is a Gartner-defined concept, a framework that comprises the interconnection of network and security components in a cloud-delivered model to meet organizations' digital and security needs.

In the security sphere, common components include:

- **Secure Web Gateways** (**SWGaaS**) for web protection, policy application and reporting
- **Cloud Access Security Brokers** (**CASB**) for sanctioned and unsanctioned cloud application protection, and data protection
- **Cloud Security Posture Management** (**CSPM**) to continuously improve and remediate cloud configurations resulting in risk reduction of probability of incidents and data losses
- **Zero Trust Network Access** (**ZTNA**) which provides secure remote access to legacy data centre or IaaS apps with benefits including reduced network attack surface, least privilege application access, and reduced risk of lateral movement
- Browser Isolation for a zero-trust approach to addressing web browsing risk

"With SASE, organizations are enabling remote connectivity resilience and security for an increasingly distributed workforce. Organizations benefit from the advantages of convergence, cloud scale and security visibility with a focus on technologies that secure users, devices, data, networks, and cloud applications."

References

*www.pulsesecure.net/resource/2020zero-trust-report

Innovations in eDiscovery

Moving to the Cloud

Pernilla Smyth

Manager
Data Management and
Forensic Technologies

eDiscovery professionals have long grappled with how to better store, search, and review electronically stored information (ESI) for litigation and regulatory investigations. We've come a long way since the early days of sifting through mountains of paper, manually reviewing every document, and figuring out how to utilize cumbersome and inefficient software. As organizations of all shapes and sizes are rapidly adopting and moving to the Cloud, the notoriously risk-averse legal world is finally joining the party.

Here are the top three innovations happening as eDiscovery migrates to the Cloud:

1. **Subscription-based, self-service eDiscovery programs are growing**
   Moving to the Cloud opens a whole new world for eDiscovery as organizations gain more control over their eDiscovery programs, while facilitating third parties to manage and store data on their behalf. This arrangement allows both corporations and law firms to get a better handle on their eDiscovery costs and easily have the option to instantly scale up or down as cases naturally change, while leaving the data security and maintenance burden with their eDiscovery service provider. Meanwhile, the Cloud lends itself to solving the perennial issue of unpredictable costs in eDiscovery as service providers are starting to embrace subscription-based services to help companies better handle costs and operate with the most up to date technologies at the same time.

2. **Artificial Intelligence (AI) and Analytics tools are more accessible and easier to adopt**
   The Cloud has many benefits, not least of which is the scalability of the services offered (e.g. storage, computational power etc.). This is particularly useful in eDiscovery as the volume and types of electronic data that must be dealt with in litigation, regulatory investigations, and even data protection assessments, continue to grow. Because of this, using AI and Analytics software to automatically decrease data sets is no longer an option but a necessity to efficiently manage complex cases. The Cloud makes AI and Analytics tools much more accessible and has the potential to transform the eDiscovery industry's typical workflows. Early Case Assessment (ECA) is one area that's particularly seeing innovation as data can be automatically categorized before it ever makes it to the review stage.

3. **COVID-19 will fundamentally alter the practice of law**
   The information governance and data management side of the EDRM has already become increasingly prominent as data exponentially grows in volume. As organizations move to the Cloud and focus more on getting their electronic data organized to mitigate cost and risk once eDiscovery becomes an issue, they will benefit from a proactive approach to data management. As was evident in the aftermath of the global financial crisis a decade ago, the volume of legal proceedings accelerated to a new level during this recessionary period. Similarly, the recession caused during the ongoing pandemic will inevitably increase post COVID-19. Companies will need to be prepared for equal levels of litigation and ensure that their data management strategies are in order.

At BSI, we've fully embraced and adopted the Cloud for eDiscovery and migrated to RelativityOne. Our clients are reaping the benefits from enhanced security, modern innovation, and improved performance.

How to improve your email security posture?

Addressing emerging trends

Michael Green

Senior Cloud Security Consultant – Security Technologies

Securing email is the most cost-efficient maximum impact step to minimizing vulnerabilities that organizations can take. Verizon's 2020 Data Breach Investigations Report revealed that phishing was the top threat action variety, meaning that it is critical to the business that your email security posture is hardened.

94%
of malware arrives on computer systems via email*

The shift from bulk campaigns to targeted attacks will continue as the technology improves and open source intelligence on organizations and their employees remain easily accessible. Phishing is evolving and a strong foundation is required to ensure readiness in the face of change and uncertainty, whether that be a manual attack, a bulk campaign, or a machine learning-enabled artificially intelligent blockchain botnet. We will now explore nine actionable steps that should be implemented to improve your email security efforts:

1. **Adaptive MFA implementation for email access**: The username and password pair are insufficient to protect against threats including password spraying, reused and leaked credentials. Multi Factor Authentication (MFA) should be utilized as a foundational component of your identity strategy and a layered defence is important here to defend against post-authentication threats. Stop using SMS as a second factor.

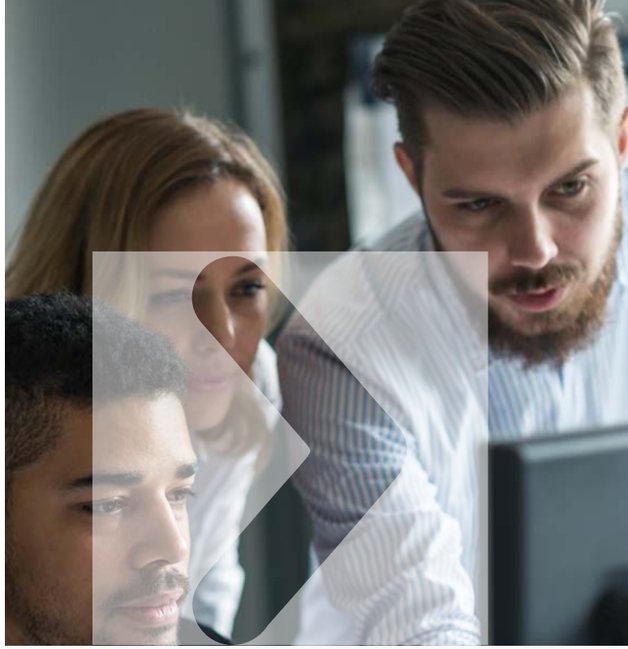
2. **Security awareness training**: Humans are often the weakest link in the security chain. Educate your workforce around the kind of threats seen in the wild in preparation for real attacks. Identity is the new perimeter and phishing can often be the path of least resistance for an attacker.

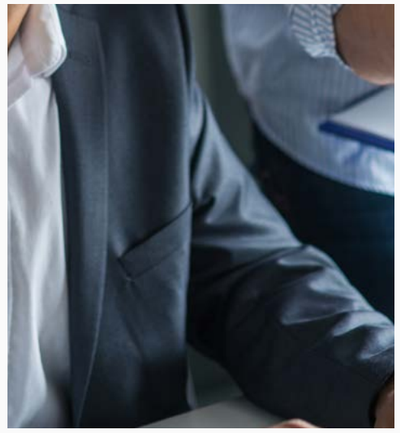
3. **Controlled phishing simulation**: Assess your posture based on real-world themes and assign additional controls where required, for example additional training to improve resilience, or adaptive hardening based on risky actions or current or impending threats.

4. **Correct and well-managed email authentication implementation (DMARC, DKIM, SPF)**: Attackers are impersonating members of your workforce for criminal gain. Proper implementation of email authentication (validating the authenticity of the domains and the emails themselves) is challenging as there is a real risk of blocking legitimate email flow.

5. **Implementation of an email security solution that is capable of and configured to address the email security risk in line with the organizations risk appetite**: Customer due diligence into the solution capabilities is key here. Review and plan to migrate away from legacy protocols in use and ensure that you have visibility and control over third-party connected cloud apps that your workforce may be allowed to grant permissions to. Other features to assess as part of your product due diligence include link and attachment scanning, cloud sandboxing, threat intelligence feeds, and third-party integrations with your existing stack.

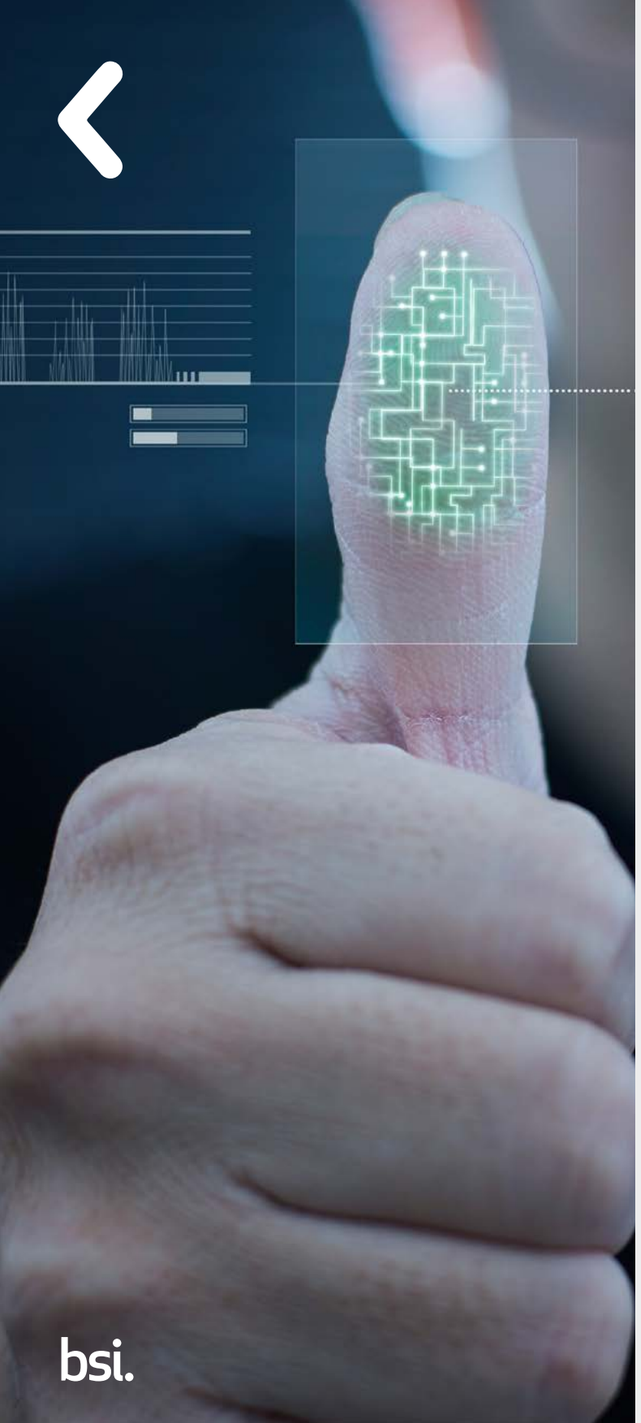
6. **Incident Response**: You should have visibility of incidents, with appropriate logging, monitoring, asset management, and visualization in place to enable this. Confirm via simulated events that you are able to respond quickly and effectively to incidents as they happen. Data-driven predictive





References

*https://enterprise.verizon.com/resources/reports/dbir



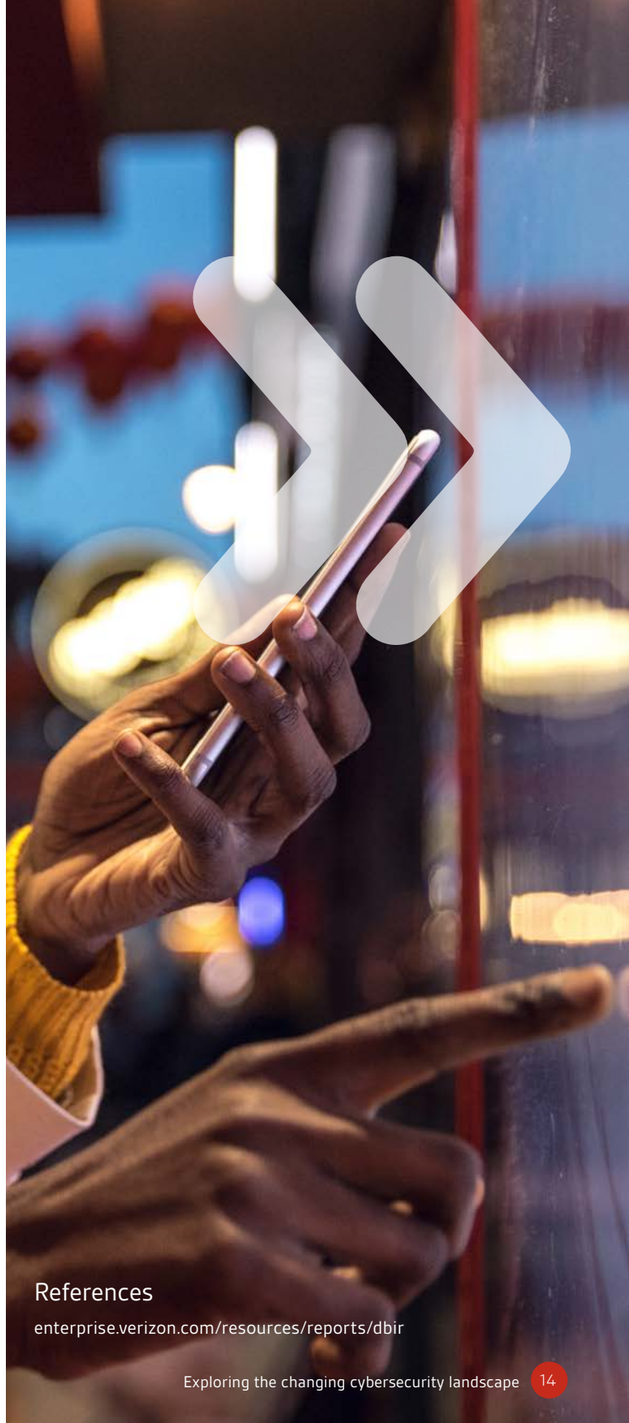
capability to proactively address and harden against potential threats should be added to your cache of tools if not already in place. A formal system of review including lessons learnt is key to ensure that posture is improved post-incident, and that incidents are properly documented and assessed, so you will be able remediate any identified gaps or issues.

7. **Email information protection**: Use email Data Loss Prevention (DLP) and integrate it with your other DLP tools. Have a well-considered data categorization/classification policy and ensure organization-wide awareness and buy-in.

8. **Email data protection**: Assess your ability to restore email data on demand with sufficient granularity. Consider malware, and malicious or accidental deletion. Ensure that your data retention and restore point frequency and availability are in line with internal and external needs. Investigate compensating controls in the form of third-party solutions, should gaps be discovered between the capabilities of the native offering and the business, operational, regulatory, and compliance requirements.

9. **Web filtering**: Having an appropriately advanced cloud-hosted Secure Web Gateway can compliment your email security solution and significantly reduce risk to your organisation. Blocking of botnets, command and control traffic, known bad or recently registered domains can be very useful as can the ability to push uncategorised domain traffic through browser isolation. Attacker use of encryption is always increasing, so you need the ability to decrypt TLS traffic at your gateway, in a scalable and sustainable manner.

There are various considerations for email security, with prioritization based on risk and impact advised, along with a layered approach. The above is not an exhaustive list but is a strong start in significant improvement of posture. In the case of cloud-hosted email, a firm understanding of your provider's shared responsibility model and your responsibilities is critical.



References

enterprise.verizon.com/resources/reports/dbir

The evolution of ransomware

John Hetherton

Global Practice Lead – PCI DSS

According to Cybersecurityventures (2020), Ransomware is expected to attack a business every 11 seconds by the end of 2021. This was every 40 seconds back in 2016 highlighting the frequency of attacks and worrying upward trajectory and trend. What are the costs of this? Cybersecurityventures outline that global ransomware damage costs predicted to reach $20 Billion (USD) by 2021.

According to the UK's National Cyber Security Centre (NCSC) and their annual incident trends report, since the well documented WannaCry and NotPetya attacks a couple of years back, ransomware attacks against enterprise networks have continued to rise in number and sophistication. Small, medium and large organizations across all sectors of industry, academia and government are regular targets.

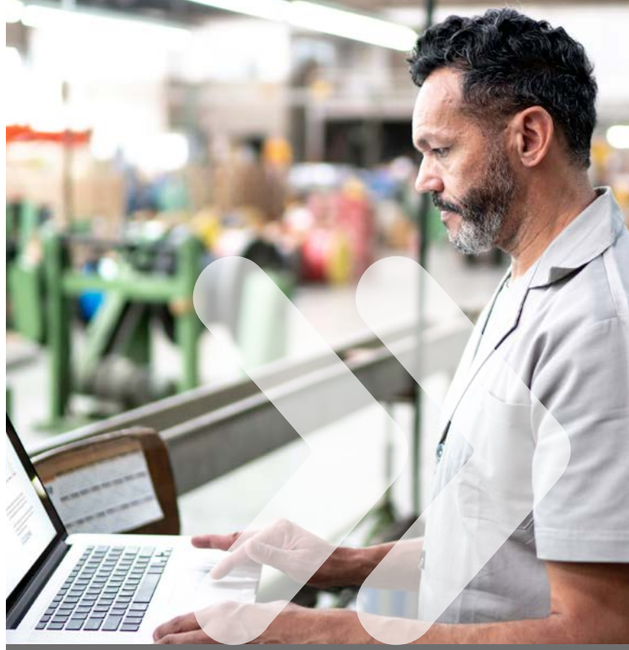
The trend for 2020 very clearly showed that lack of conscience of ransomware operators. What started out as a commodity attack, similar to traditional malware, soon evolved when the power Ransomware could wield became clear. Attackers levelled up to combine traditional attack skills (Phishing, RDP brute force, network vulnerability exploitation) with ransomware to maximise return on investment.

Intensive reconnaissance and network enumeration became the norm, where active attackers penetrate the network, identify critical servers, use of weak shared credentials and locations of back-ups to ensure highly effective targeted attacks. New techniques to shorten time to pay begin to leverage brand and reputational impact, with attackers exfiltrating key data sets before encrypting, and posting samples on-line and threatening full disclosure of an organizations data.

Where we see the real unscrupulous nature of the ransomware attacker is evident in the focused attacks on healthcare during the global pandemic; a hospital succumbing to ransomware in Germany and having to divert ambulances to other hospitals, mental health clinics being compromised and individual extortion attempts being levied on patients of the clinic, and evidently a large proportion of the UK NCSCs time being spent, helping increase health services provider cyber resilience.

Given how lucrative ransomware is we are likely to see more of the same, however we should all expect, that like any organization, where there is profit additional focus will be spent to capture the market. More resources, will leverage more exploitable systems as organizations struggle to move off highly consumed and now deprecated platforms like Windows Server 2008.

$20b (USD)
Global ransomware damage costs are predicted to reach $20 Billion (USD) by 2021*



"For cybercriminals, the 'cyber-world is their oyster' and an obviously lucrative one – until we as defenders do a better job of preventing these ransomware attacks, we can expect this business to be very popular domain for these threat Space."

References

* Cybersecurityventures: cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021

National Cyber Security Centre: www.ncsc.gov.uk/report/incident-trends-report

Machine learning in offensive cyber operations

Muath Sharawi

Global Practice Lead – Network Testing

Adversaries employ different automation techniques throughout the attack lifecycle. As these techniques have seen much success in delivering highly sophisticated attacks in recent times, Machine Learning (ML) is expected to evolve in relation to offensive operations in the short-term, namely in the areas of social engineering and defence evasion.

55%
of global organizations experienced a successful phishing attack last year*

Research around the utilization of Machine Learning (ML) in adversary offensive operations is still at its very early stages. However, current studies and trends show that ML has seen several phases of the attack lifecycle become more sophisticated, resulting in an increase in the scale, success rate, and impact of adversary operations.

One of the main areas expected to benefit from ML is social engineering. According to Proofpoint's 2020 State of Phish report, 55% of global organizations experienced a successful phishing attack last year. This success rate of malicious attacks is likely to increase with the incorporation of ML techniques.

Currently, there are tools that can generate unique realistic human faces (for example StyleGAN by NVIDIA), create quality longform content that is coherent, realistic, and can mimic the style of a particular author (GPT-3 by OpenAI), in addition to the ability to create synthetic human voices to imitate a particular individual (Tacotron by Google). These tools are likely to increase the sophistication, breadth, and success rate of phishing campaigns against organizations and decrease the effort required to run them.

Another practical area of interest is defence evasion. Through the usage of ML, a threat actor's payload might be able to more accurately identify when it is running in a sandbox environment for a security tool and change its behaviour accordingly, therefore increasing the attacker's chances of a successful initial foothold into the target organization by bypassing the implemented security tools including spam filters, anti-virus and intrusion detection systems, among others.

Other aspects of offensive operations are not expected to benefit from ML in the short-term as current automation tactics used by threat actors would suffice. This may change in the long-term as ML becomes more accessible with evolved abilities. Nevertheless, we expect to see more ML driven offensive operations in 2021.

"Machine learning tactics are likely to increase the sophistication, breadth, and success rate of phishing campaigns against organizations."

References

*www.proofpoint.com/sites/default/files/gtd-pfpt-uk-tr-state-of-the-phish-2020-a4_final.pdf

github.com/NVlabs/stylegan2

cset.georgetown.edu/research/automating-cyber-attacks

google.github.io/tacotron

openai.com/blog/openai-api

What happens when you mix blue and red?

Jeremy Newby

Head of Practice, CSIR Global Security Testing

Security testing is the art of utilizing offensive testing techniques to verify the effectiveness of existing security controls and verifying the full impact of any identified vulnerabilities should they be exploited by a malicious attacker.

Organizations who long boast about strong security controls and processes may not be able to detect and contain a breach immediately. For example, 146 days is the average time hackers stay hidden on a network, which is a long time for threat actors to learn and understand many of the confidential details and privileged information of the company. If organizations do not practice regimental detection and response capabilities and their security teams are not prepared for the inevitable, the likelihood of effectively executing them in a real breach scenario is minimal.

What we are seeing moving into 2021 and indeed what was witnessed in 2020, is organizations investing in not only attack and adversary simulation (Red teaming) but also defensive techniques (Blue teaming) and Purple teaming. Purple teaming is the hybrid security methodology and approach where both red and blue teams are inextricably in offensive and defensive security testing techniques, working harmoniously to maximize the information resilience capabilities through continuous feedback, knowledge transfer and adoption of best practice.

Purple teaming as a concept and an approach can be a particularly powerful one, often with training of the Blue Team being a key objective, which in turn drives improvement throughout an organization and tightens its defences. Additionally, a Purple Team engagement does not necessarily need a high level of organizational maturity to be able to see actionable results due to the direct and collaborative approach which is not always the case with a Red Team. Purple Teaming is often seen as a sensible, pragmatic approach to proactive security and, along with Red Teaming, is the only testing type which truly gives a picture of the level of preparedness of an organization to resist a cyber-attack.

There are various schemes introduced to the market which support and mandate this type of work, for example the CREST STAR accreditation, the CBEST scheme from the Bank of England and others outside the UK including TIBER-EU and iCAST. There was also the introduction of the GBEST scheme for government departments. Ultimately, what these schemes and accreditations achieved was to formalize the market requirement and mandated that organizations in certain industries had a duty to carry out such engagements.

As more industries and sectors realize the benefits of performing attack simulation tests, BSI believe that the popularity of Purple Team testing will continue to rise as it did during 2020 and into 2021 beyond.

146
days is the average time hackers stay hidden on a network*

"In the coming year, we foresee organizations investing not only in adversary simulations but also in defensive security testing."

References

*Hackers stay hidden on a network www.microsoft.com/en-us/cloud-platform/advanced-threat-analytics

Find out more

EMEA
Call: +353 1 210 1711
Email: cyber.ie@bsigroup.com
Visit: bsigroup.com/cyber-ie

UK
+44 345 222 1711
cyber@bsigroup.com
bsigroup.com/cyber-uk

US
+1 800 862 4977
cyber.us@bsigroup.com
bsigroup.com/cyber-us

Subscribe to our newsletter

Follow us on

BSI Group, Corrig Court, Corrig Rd,
Sandyford Business Park,
Sandyford, Dublin

T: +353 1 210 1711
E: **cyber.ie@bsigroup.com**
Visit: bsigroup.com/cyber-ie