Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company’s public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
tests and IT health checks as you would do for all solutions.

Enable the IT security community

New and agile competitors are coming in and eroding market share or even creating new markets, such as Uber and Airbnb. This means that fostering business agility is essential to survive and prosper. This is where the modern CISO can really make a difference by leaning into the development process and driving a shift-left culture. There are three important steps to drive this culture change.

Educate: In the same way that you have been educating yourself as the CISO, your teams need to be educated. As we have previously mentioned, it is very difficult to know everything. However as a starting point it’s recommended that the IT security teams should build their knowledge in the following key concepts:

- Software defined networking (SDN) and zero-trust architecture.
- Disk and network encryption.
- Key and certificate management.
- Cloud network security devices.
- Policy management.
- Identity and access management (IAM).
- Public and private interfaces in the public cloud.

Embed: You should adopt the cross-functional team concept by embedding empowered security personnel into engineering teams. But what do we mean by empowered security personnel? These are people who have delegated authority and knowledge to make relevant security decisions that are within the bounds of the project. Wider decision-making that impacts across the enterprise will still need to go through a security governance process for approval.

Evangelise: The final task on the journey is to educate the wider business community and be seen to champion IT security and how it can empower the business. This can be with knowledge sessions, developing learning paths and creating a security community of practice.

Conclusion

As IT has embraced the latest innovations of public cloud and DevOps ways of working, is it time for you to make a sea change as well? The journey to becoming a modern CISO is rooted in trust – trust the cloud and CSPs and enable the IT security teams and community to drive change.

Championing the security shift-left approach, to promote the shipping of secure and compliant solutions, will enable greater business agility during these times of change.

About the author

Olivier is an account principal at Contino, working with enterprise customers to achieve business value through digital transformation. He has significant experience in strategy, digital transformation, enterprise and IT infrastructure consulting, technical leadership, project management, cloud and DevOps technologies across a number of industry sectors. He also has extensive experience of establishing and structuring complex technology-enabled business transformation projects using traditional and modern methods.

References

1. ‘Cloud computing with AWS’. Amazon Web Services. Accessed Sep 2020. https://aws.amazon.com/what-is-aws/?nc2=h_ql_le_int.
2. ‘Azure products’. Microsoft. Accessed Sep 2020. https://azure.microsoft.com/en-gb/services/.
3. ‘Google Cloud Platform Services Summary’. Google, 15 Sep 2020. Accessed Sep 2020. https://cloud.google.com/terms/services.
4. ‘Audit Report’. Microsoft Azure Trust Portal. Accessed Sep 2020. https://servicetrust.microsoft.com.
5. ‘AWS Artifact’. Amazon Web Services. Accessed Sep 2020. https://aws.amazon.com/artifact/.
6. ‘Compliance Resource Center’. Google Cloud. Accessed Sep 2020. https://cloud.google.com/security/compliance.

How to leverage data security in a post-Covid world

Andrea Babbs, Vipre Security

Cyber security is often pushed down the list of priorities, and this was abundantly clear as businesses had to rush to get employees up and running for business continuity in recent months. Many already had some level of protection in place, but with a lasting switch to remote working and changing work habits and practices, there must be a refreshed emphasis on data security to protect employees, customers and businesses.

IT security leaders have already seen a 30,000% increase in Covid-19 themed attacks as, unsurprisingly, cyber criminals took advantage of the situation – and they won’t stop.1,2 As many workforces are more decentralised, this highlights that there is an even more important need for employees to take responsibility for protecting data.
The risks

With changes to work patterns and styles, such as the move to remote working, there is no longer scope for easy peer review and questions. Employees are making critical security decisions on their own and many may not reach out to colleagues to ask simple questions, such as, ‘does this email look strange to you?’. It’s widely documented that phishing scams are one of the most common ways for cyber criminals to attack businesses and data, and with employees eager to show managers that they are working effectively remotely, it may mean crucial errors aren’t picked up. After all, email is the number one threat vector in organisations and the cause of nearly all data breaches, as confirmed by the Identity Theft Resource Centre. Moreover, the Information Commissioner’s Office (ICO) found that misaddressed emails are the largest source of data loss for organisations – with over 269 billion emails sent around the world each day.

Gone are the days when employees operated from a single office-based computer. The modern workforce is now working from potentially several locations across a number of devices. Furthermore, employees are increasingly trusted with company-sensitive information, assets and intellectual property. Many are permitted to make financial transactions – often without requiring any further approval. Given the data protection requirements now in place, not only as a result of the General Data Protection Regulation (GDPR) but also industry-specific regulation, as well as accountability to internal compliance teams, organisations clearly require robust processes and savvy employees to mitigate the risk of inadvertent data loss.

Businesses need a clear strategy to address the issue of misaddressed emails and mitigate the associated risks to remain compliant and secure. But is a strategy that simply imposes stringent penalties — including dismissal — on employees for mis-sent emails without providing any form of support actually going to foster a positive culture? What employees require is consistent training and a way to better manage email, with a chance for potential mistakes to be flagged before an individual hits Send.

Protecting data from within

According to Forrester, 53% of data breaches are classified as insider, so clearly the workforce has a critical role to play in an organisation’s cyber defence strategy. There is a solution that can add a layer of employee security awareness — for example simple safety checks that give email users the chance to confirm the identities of email addressee(s) and, if present, attachments. It can also help employees avoid common mistakes like missing off the attachment altogether. These types of solutions can provide that layer of data protection while also improving efficiency.

These solutions can also verify domains to allow for unchecked internal emails if allowed by the company, or the solution can be deployed on a department-by-department, even user-by-user, basis. For instance, a business may not want HR to be able to mistakenly send sensitive personal information to anyone internally and therefore require a confirmation for all emails. Similarly with financial data, even marketing data at certain times — such as in the run up to a highly sensitive new product launch.

The technology can also check for keywords within the email and this list can be personalised to the business to include specific phrases but also common terms such as confidential, private, credit card numbers or National Insurance/Social Security numbers. Any emails — including attachments — containing these key words — or, for instance, unreleased product names — will be flagged, requiring an additional confirmation before they are sent, and giving users a chance to double check whether the data should be shared with the recipient(s).

This approach provides an essential ‘pause’ moment, enabling individuals to feel confident that emails have been sent to the right people and with the right attachments. An essential tool in the fight against phishing emails — for example, an email that purports to come from inside the company, but actually has a cleverly disguised, similar domain name. If a busy employee responds to an email from V1PRE, for example, as opposed to VIPRE, thinking it genuinely comes from inside the business, the technology will automatically flag that email when it identifies that it is not an allowed
domain, enabling the user to cancel Send and avoid falling for the phishing attack.

Expanding cyber security

High quality, layered protection must cover web and endpoint protection as well as email security: there is an increasing number of attacks happening each year and criminals are getting more sophisticated. Businesses must match this evolution and ensure that every part of the business is protected. Cyber security tools have never been more important.

As identified, employees are the number one threat to businesses through human error: however, by focusing on the user and ensuring proper education, businesses can empower employees with the confidence to take on responsibility for data security, leading to a better protected organisation. Memorable, bitesize chunks of training, regularly spread throughout the year is key to making every employee an honorary member of the IT security team.

This adaptation will ensure that everyone in the business is working to protect data, both their own and customers’. Should confidential corporate information fall into the wrong hands, the consequences could be devastating, including reputational damage, intellectual property loss or compliance breaches, which businesses must be aware of when deciding how much to invest in their IT security infrastructure. Crucial company information such as proprietary ingredients or the blueprints of an unpatented new product leaking into the public domain could easily be intercepted by the competition, resulting in a lost competitive advantage.

All it takes is a simple missed or added character in the email address, autocorrect taking over, or simply pressing Send too soon and the information that was once confidential is sitting in the wrong inbox. It could be that of an unknown individual, competitor, or even a cyber criminal.

High cost

The cost is certainly high, with data breaches reaching considerable sums in fines – for instance, the case in 2018 where the Independent Inquiry into Child Sexual Abuse (IICSA) was fined £200,000 by the ICO for failing to protect the identity of possible victims of child abuse after a human error accidentally exposed victim identities to third parties, when they included their email addresses in the ‘To’ rather than ‘BCC’ field.6 This demonstrates just how seriously the ICO takes these types of data breaches, and the pain of embarrassment from sending an email to the wrong contact pales in comparison to the business pain from financial penalties.

While accidentally calling a wrong number can be a little embarrassing, the same cannot be said for sending an email to the wrong contact. You could try to correct the error with a follow-up email to apologise and request that the recipient delete the message, but even if you’ve spotted the error it’s often too late. Moreover, the misuse of CC and BCC functions could expose your entire contact database, potentially giving your competitors an opportunity to lure your customers or employees away, or worse – exposing customer emails to potential hackers.

BitMEX, one of the world’s largest crypto-currency trading platforms accidentally leaked thousands of private customer email addresses when they sent out a mass mailshot without using the BCC function.7 While the company maintains that customer privacy remains a top priority, its customers were left wondering how they could trust BitMEX with huge personal assets in the aftermath of this data protection failure.

Returning to ‘normal’

As businesses slowly move back to normality and employees start to return to office spaces – albeit in a different way
from before – it’s clear that businesses must make sure they don’t compromise on security. The new normal of hybrid workforces must have the correct layers of security that protect all types of employees, for example with a combination of reminders, prompts and continuous training to go alongside technology solutions.

Employees no longer have to be the number one threat to business security – they can instead be a vital tool in the fight against cybercrime, with access to regular training backed up by technological solutions that support and catch the inevitable human errors. By enabling users to make informed decisions about the nature and legitimacy of their emails before acting, without adding time or delay to employees that are already under pressure, organisations can mitigate against this, while reinforcing compliance credentials. It’s about increasing awareness and improving email culture where mistakes can so easily be made, and helping business leverage efficiency and continuity post-Covid.

About the author
Andrea Babbs has worked in the IT industry for more than 20 years. She is country manager and head of sales for Vipre Security, managing the UK and Irish business. Her industry experience means she has seen the threat landscape change from simple viruses to the sophisticated threats of today. She recognises that humans are the last line of defence, meaning they need awareness and effective tools to help them prevent little mistakes with big consequences.

References
1. Muncaster, Phil. ‘Experts Detect 30,000% Increase in #COVID19 Threats’. InfoSecurity, 27 Apr 2020. Accessed Sep 2020. www.infosecurity-magazine.com/news/experts-detect-30000-increase/.
2. Desai, Deepen. ‘30,000% Increase in COVID-19-Themed Attacks’. Zscaler, 23 Apr 2020. Accessed Sep 2020. www.zscaler.com/blogs/research/30000-percent-increase-covid-19-themed-attacks.

PKI is key to securing a post-Covid remote workforce

Brian Trzupek, DigiCert

In just a few short months, the Covid-19 outbreak has dramatically changed the way that global employees work. In a recent IDC survey, respondents said they expect nearly 30% of their workforce will be working from home in 2021, compared to approximately 6% of their workforce prior to the pandemic.1

Analysts estimate that we have witnessed two years of IT digital transformation in two months, and many of the changes are here to stay. According to Gartner, 74% of CFOs expect to permanently transition many employees to remote work.2 Yet as security admins renew their focus on scaling out deployments to a newly remote workforce, many of their usual challenges remain. They want to be sure their infrastructures are configured correctly to allow the right people in, with access to the right tools, data, and resources they need to stay productive. At the same time, they need to keep bad guys out and keep users in restricted areas if they require only limited access.

Security admins are also focused on choosing solutions that can scale most effectively across their user base and putting plans in place to discover and fix issues if their solution misbehaves.

Agile and secure

The Covid-19 healthcare crisis emerged rapidly, and most organisations were forced to shift employees to remote work in just weeks or even days. The switcher has opened the door to a flood of new security threats. Spear-phishing attacks, as well as other direct employee compromise attacks, are on the rise. Unlike typical phishing attacks that are usually sent to mass emails, spear-phishing attacks are aimed at specific individuals, or small, precisely targeted groups. The rapid