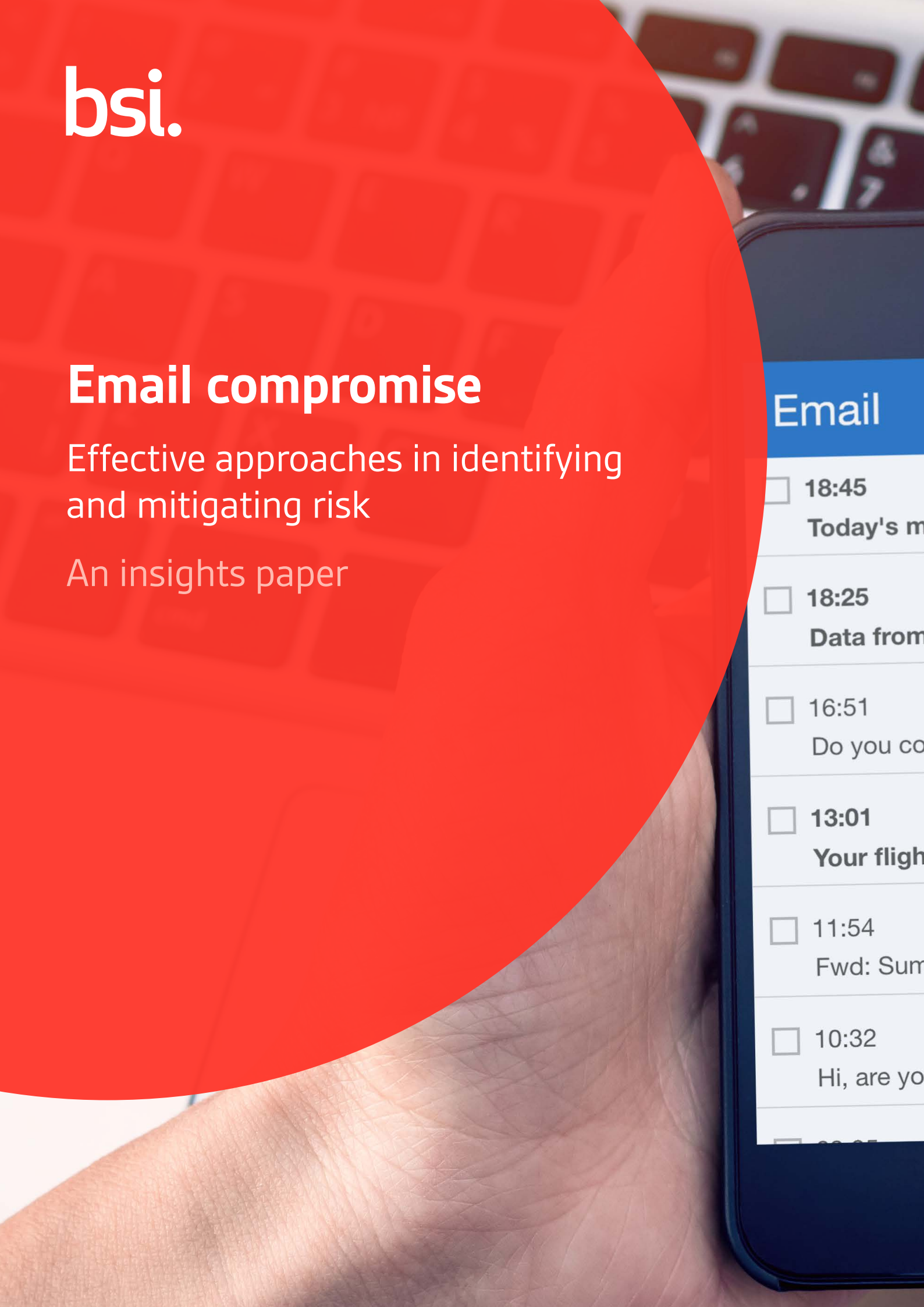
bsi.

Email compromise

Effective approaches in identifying and mitigating risk

An insights paper



Executive Summary

Email is deeply embedded in our society and represents a core technology in facilitating global collaboration and business growth. However, organizations need to be aware of the security risks involved to be able to effectively govern its secure use. Email is the number one threat vector with more than **90% of cyber-attacks starting with email** as documented in the 2019 Data Breach Investigations Report by Verizon. Email is not a 'set and forget' technology rather it requires continuous optimization to reduce the risk of compromise.

Email compromise can result in heavy financial losses, with the FBI publishing victim complaint report figures of international and domestic **US losses of $26 billion** between 2016 and 2019[1].

We break email compromise into two common types:

1. **Business Email Compromise (BEC)**. The attacker pretends to be the victim or related party via technical manipulation
2. **Email Account Compromise (EAC)** refers to an attacker compromising an account, masquerading as the victim.

We will now look at BEC, EAC, and selected controls for risk reduction.

Business Email Compromise (BEC)

There are three common types of BEC as described below:

1. **Domain Spoofing**
   The attacker would send an email that appears to come from your domain. This is possible because the Simple Mail Transfer Protocol (SMTP) does not have the ability to authenticate email messages and requires additional technologies such as SPF, DKIM, and DMARC to do this.
2. **Similar Domains**
   The attacker registers a similar domain, perhaps with a 1 instead of an L, likely rendered in lowercase in an email client or browser. This could then be used to trick the victim into believing that the message was in fact a legitimate email from a colleague, partner, or customer.
3. **Display Name Spoofing**
   The attacker modifies the from: and reply-to: fields of the message header, inserting a spoofed trusted sender to be displayed in the email client, and an email account under the attacker's control, where replies will be sent to.

Organizations should consider internal emails, email with partners, customers, and the supply chain. An attacker could potentially pose as any one of the above entities, attempting to elicit information, to alter the flow of money, or to attempt EAC. There are several controls or steps that can be enabled to reduce organizational risk for BEC.

1 https://www.ic3.gov/media/2019/190910.aspx

Selected controls for BEC risk reduction:

Employee security awareness training

As the majority of attacks require user intervention, security awareness training should be provided either online or in person at various intervals and broken up into initial, recurring, and refresher variants, based on the requirements of the organization and its users. Simulated phishing could be used by the organisation to measure and strengthen the workforce's ability to identify and report phishing attempts. Training your users to spot display name spoofing and the use of similar domains is key. The retention of the information contained within the training can then be verified and corrected via simulated phishing, and further training, as needed.

Technical controls

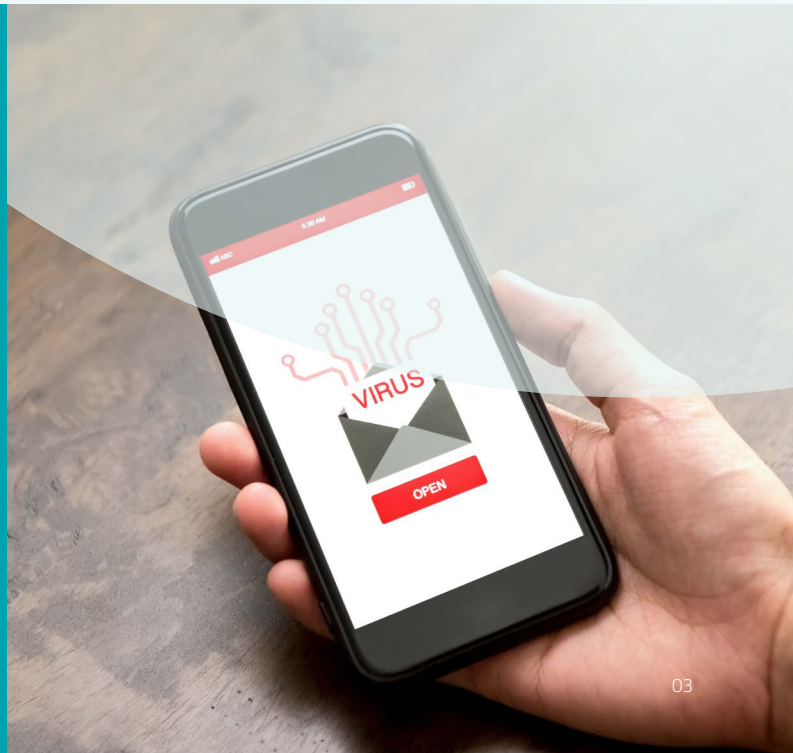
There are three technical measures that should be evaluated for use in your organization to secure email validity. Domain Keys identified Mail or **DKIM** is where the domain in an email message is authenticated via a digital signature. Sender Policy Framework or **SPF** is a check made to confirm that the mail server is authorized to send mail from the domain. Domain-based Message Authentication, Reporting, and Conformance or **DMARC** allows the organization to protect their domains, via the control and reporting of the application of DKIM and SPF. There are complexities when implementing these technologies and we recommend that a full analysis is completed to ensure to minimize false positive results and to ensure that valid email is not impeded.

Other technical controls including threat intelligence, machine learning, and artificial intelligence which could form part of your current or future vendors product offering. The benefits of email compromise-based information sharing will result in risk reduction and a higher ROI.

Your chosen solution may also offer elements of control and additional visibility around the threat of display name spoofing, and the use of similar domains. Your Secure Web Gateway or DNS security solution may enable you to control access to newly registered domains by your workforce. This can be useful to reduce the risk of similar domains as a phishing threat and you may also have the capability to block known phishing sites.

What we have seen is that DMARC adoption is low due to the aforementioned complexity and there is room for more organisations to implement it, to increase the security and trustworthiness of the domains that they own. Your organization should review not only the status of your own domains, but also those of your partners, customers, and parties in your supply chains. This information is publicly available. This is also a threat.

Simulated phishing could be used by the organization to measure and strengthen the workforce's ability to identify and report phishing attempts.



Email Account Compromise (EAC)

As mentioned previously, EAC refers to an attacker taking over an email account. A phishing email may be sent to the victim, where a link is clicked on and the victim is redirected to a malicious site that may resemble or have cloned a portal that the victim uses daily. The victim may then enter their credentials into a web server under the attacker's control.

In addition to malicious links, we need to think about attachments which could contain malicious software like Remote Access Trojans (RATs) or Ransomware.

What the attacker would then do with this access can vary. Examples include:

- The attacker monitoring the way that you write and sign off emails, to improve their ability to emulate authentic messages
- Setting up a forwarder to forward all messages to an external account of their choosing although we expect to see a reduction in the coming years as email technology evolves
- Attempting communication with internal or external resources, with the goal of financial or informational gain.

Selected controls for EAC risk reduction:

Phishing simulation can work together with security awareness training, improving, testing, and correcting your users, enabling continuous improvement, and resulting in a stronger security posture. They may even be integrated. Enabling a Multifactor Authentication **MFA** solution which adds additional factors to the authentication process can reduce the risk of email account compromise. The solution's capability around Adaptive MFA and device posture checks should also be investigated. **Email link rewriting** is where vendor solutions can make malicious emails safe via modification of content. An example of this would be rewriting malicious links. **Browser isolation** is a zero-trust approach to web browsing that executes browsing requests in an isolated environment rather than locally on a user's machine. **Application allow and block listing** is a control whereby should a user open a malicious executable or script, application allow and block listing can significantly reduce the risk that the malicious software would be able to run. Organizations should also consider policies for scripting tools such as PowerShell and whether scripts can run on the devices.

Enabling **least privilege** for user accounts minimizes the ability to install malicious software. If the user trying to install something and does not have permission to do so, then it will not be installed. Cloud identity, single sign-on **SSO**, and cloud application access also needs to be considered, as cloud email account compromise could result in non-email cloud application compromise.

Of course as and when organizations place a secure email system into place they are protected from that point on but this does not mitigate the risk that threats have already arrived into the email estate and could be activated a later point if opened. Thus, the removal of known or potential malicious emails from existing mailboxes across the organisation should be considered. There are several possibilities for organizations to consider ranging from manual scripted ones to use of appropriate third-party email extractions.

Warnings on the email client should be implemented to inform users that emails are coming from outside the organisation or have suspicious properties. For defence in depth, we can combine that with endpoint protection in the form of antivirus, endpoint detection and response **EDR**, and a secure web gateway **SWG** should be able to control and block malicious domains and content and apply appropriate policy management.

Enabling a Multifactor Authentication MFA solution which adds additional factors to the authentication process can reduce the risk of email account compromise. The solution's capability around Adaptive MFA and device posture checks should also be investigated.

Reporting

Organizations need to generate reports suitable for presentation to executives that show actionable data that can inform steps that strengthen the security posture of the organisation. Report data that should be captured should include

- Who is being attacked?
- Can we see any patterns?
- Where are the attacks coming from?
- Are they part of a wider campaign or highly targeted?
- What are the attack types?
- Do the emails contain malicious links or attachments?

Conclusion

Email security has both technical and human considerations to be addressed. On this basis, organizations should be using layered defences when designing controls for risk reduction around email compromise. There needs to be a capacity for automation and integration with other security platforms to provide a holistic defence in depth. The above information provides a selection of controls that can be reviewed, used, and implemented to mitigate BEC and EAC as needed.

Organizations should be using layered defences when designing controls for risk reduction around email compromise.

How can BSI help?

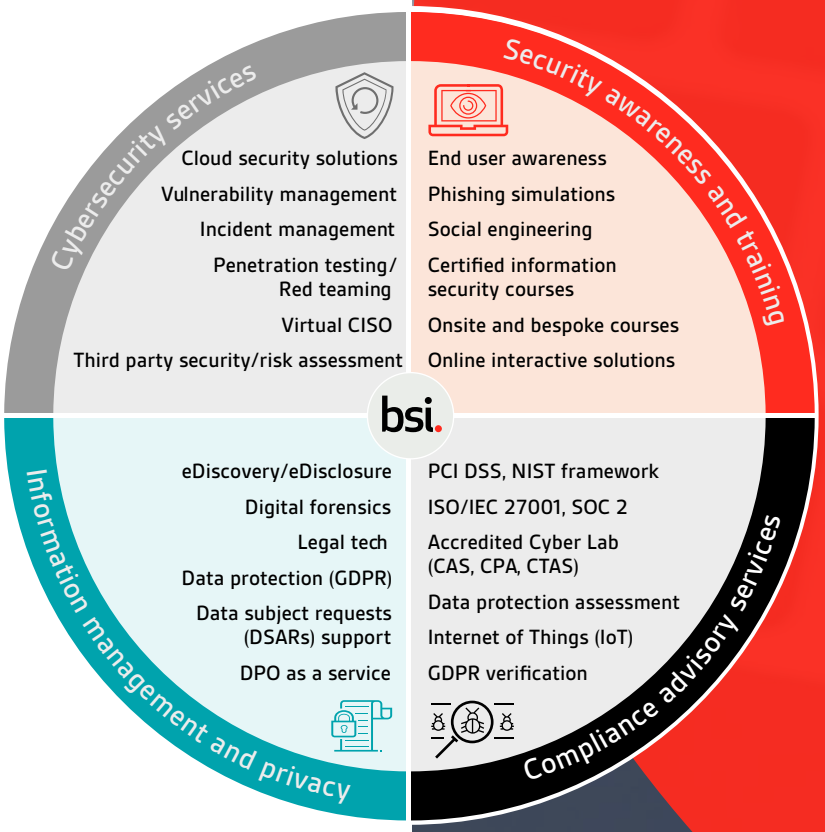
BSI partners with **Proofpoint** the Gartner Magic Quadrant leader for secure email gateway for seven consecutive years through 2020 and our consultants can engage with your organization to discuss your email security requirements and arrange a free demonstration of the Proofpoint platform.

bsigroup.com/en-IE/our-services/cybersecurity-information-resilience/Technology-solutions/cybersecurity-and-compliance-solutions/proofpoint-email-security

Protect your information, people and reputation with BSI

Expertise lies at the heart of what we do. As trusted advisors of best practice, we empower you to keep your business safe through a diverse portfolio of information security solutions. Whether it's certification, product testing, or consultancy services or training and qualifying your people, we'll help you achieve your security goals.

Our Cybersecurity and Information Resilience Services include:



Our expertise is accredited by:

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

bsi.

Subscribe to our newsletter

Follow us on