TitanHQ™

Cyber Security Awareness Assessment Checklist

As security attacks soar, planning and assessments are crucial ways to mitigate risk.

TitanHQ.com

Cyber Security Awareness Assessment Checklist

As security attacks soar, planning and assessments are crucial ways to mitigate risk. As such, a cyber security awareness assessment is integral to an organization's strategy for avoiding hackers. In addition, security awareness assessments are a way to measure the effectiveness of your security training program and provide a list of must-haves for training and technology.

TitanHQ shares our experience of delivering successful cyber security programs, looking at the elements necessary to carry out a successful cyber security awareness assessment..

The Seven Elements of a Security Assessment

The seven core elements to cover as part of a cyber security awareness assessment are:

Assessment Areas for Cybersecurity Awareness

Below, TitanHQ dives a little deeper into the elements of a security assessment:

Phishing and Spam

Phishing is the core element of a security risk assessment as it carries the most risk. According to the Cisco "2021 Cybersecurity Threat Trends Report," 90% of data breaches begin with phishing emails. Areas that require an assessment to be carried out to ensure that employees are being trained effectively are:

- Types of phishing: include email phishing, spear-phishing, Vishing, and SMShing
- Email security: tactics and tricks used to make phishing emails look legitimate.
- URL awareness: how to avoid dangerous links.
- Malicious websites and data entry phishing: educating employees on the importance of being vigilant after clicking a link in an email.
- Attachment awareness: the importance of being circumspect when choosing to download to open an email attachment.
- Social engineering: examples of how scammers manipulate and socially engineer people.

Preventative measures:

- Security awareness training
- Phishing simulation exercises
- Anti-spam technology
- DNS filtering

96%

of all phishing attacks arrive via email.

Source: boxphish.com

Security Hygiene

Security extends to every possible part of an organization, including the physical. For example, pretexting and tailgating often involve social engineering in the real world. Also, the mis-delivery of emails is a simple example of a general security error that can result in exposed data. According to the IBM Threat Intelligence report, human error contributes to 95% of cyber-attacks. Therefore, make sure that you cover the following areas:

- Data protection and destruction: do employees understand the company data security policy?
- Physical security: pretexting and tailgating often circumvent physical security barriers; ensure that employees understand how these real-world social engineering attacks happen.
- Tidy desk: a clean or tidy desk policy is a requirement for regulations such as ISO 27001. Does your cyber security awareness cover a clean desk policy?
- Password security: does your security awareness cover password policy requirements with employees? Are your training individuals on the importance of robust policy creation and MFA options?

Preventative measures:

- Security awareness training
- Robust, enforceable security policies

Mobile Security

Mobile security is vital in an age where BYOD reigns. A Checkpoint report into mobile security found that mobile malware is rising. The same report identified that 46% of organizations had at least one employee download a malicious mobile app. Ensure that your security awareness assessment covers the following:

- Clean devices: do employees understand your mobile app install policy? Are employees taught about safe apps and how to avoid malicious apps?
- Device replacement: when replacing mobile devices or other computer items, ensure that employees understand the security policy covering device replacement.
- Mobile device security: the importance of installing mobile device updates promptly
- Safe internet access: safe surfing from a mobile device.

Preventative measures:

- Security awareness training
- Phishing simulation exercises
- Anti-virus
- Robust, enforceable security policies

97%

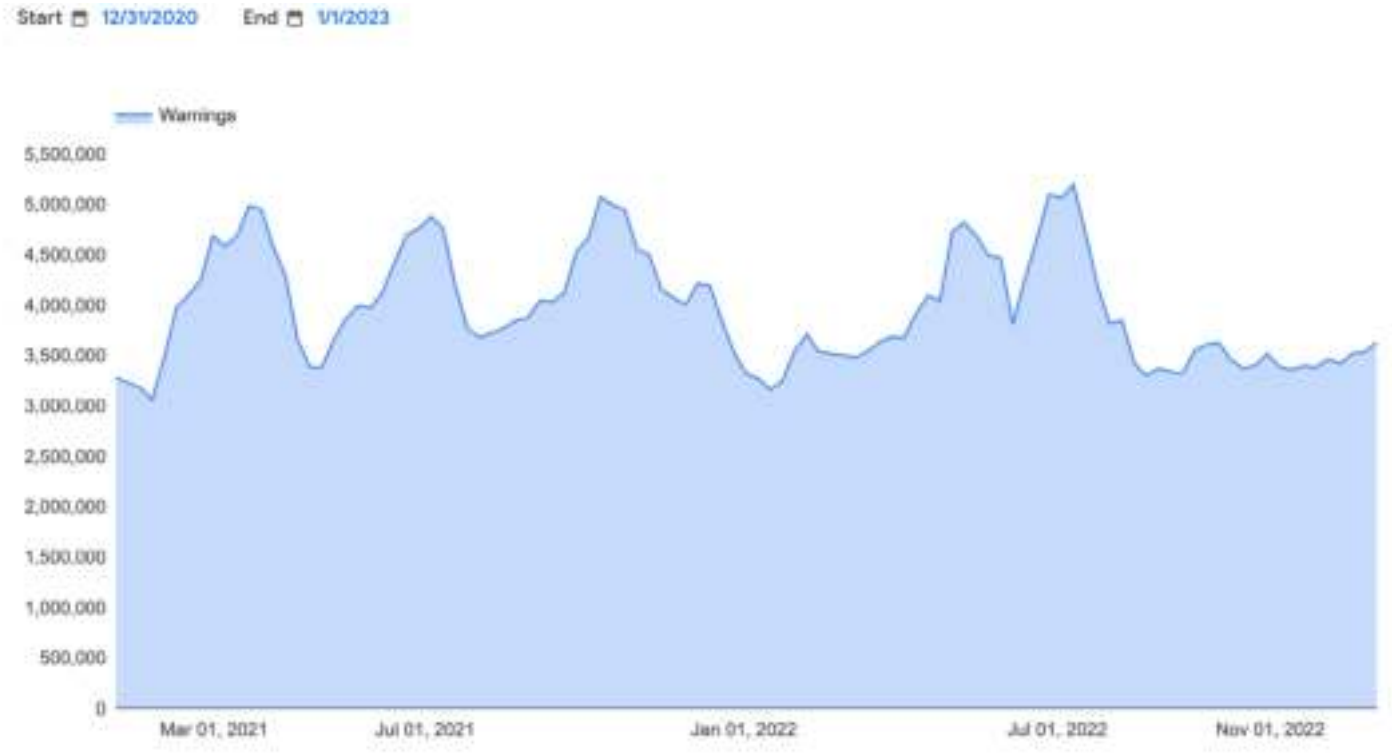
of organizations around the world have experienced an increase in email phishing attacks.

Source: www.cybertalk.org

Navigate Online Safely

Phishing websites and infected URLs are common. According to Google's Safe Browsing statistics, on January 1st, 2023, Chrome issued over 3.6 million warnings. In Q3 2022, the Anti-Phishing Working Group detected 415,630 unique phishing websites. Make an assessment checklist for the following to ensure online safety:

- Safer web browsing: spot the tell-tale signs of a malicious website.
- Awareness of data entry: are employees aware of how fraudsters steal login credentials and other data using phishing websites?

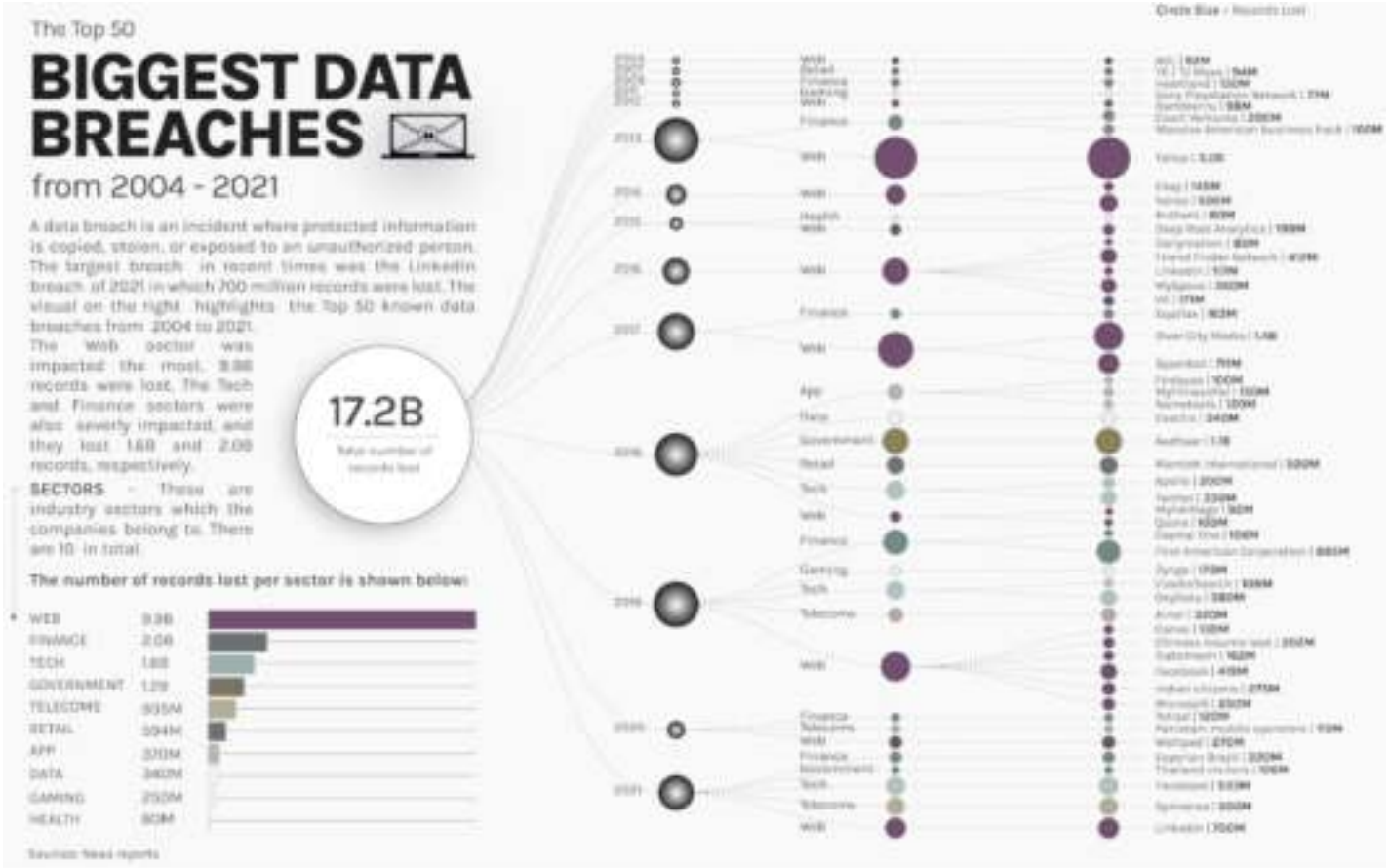


Preventative measures:

- Security awareness training
- Phishing simulation exercises
- DNS filtering

Protecting Personal Data

Personal data is a honeypot for cybercriminals. So protecting personal data is an essential part of regulatory compliance too. Visual Capitalist research shows that 17 billion data records were stolen between 2004-2021.



Ensure your cyber awareness assessment covers the following:

- Personally Identifiable Information (PII): what is it, and how should it be protected
- Data protection and destruction: what role does an employee play in ensuring secure data destruction.
- Personal data awareness: how to stop personal data from leaving the organization, including via email and social media.

Preventative measures:

- Security awareness training
- Security hygiene training
- DLP (data loss prevention) technology

Remote Working Security

Since the Covid-19 pandemic, remote and hybrid working has become normalized. A Malwarebytes report found that remote work was behind data breaches in 20% of organizations. A cyber security awareness assessment must check that you have included remote work as a possible source of a cyber breach; include in the assessment:

- Remote work security policy: does our organization train employees who work remotely on how to secure devices, etc.?
- BYOD security: has the employee the tools needed to secure home devices, including printers?

Preventative measures:

- Security awareness training
- Simulated phishing exercises
- Anti-spam technology
- Security hygiene training
- DLP (data loss prevention) technology
- DNS filtering
- VPN or similar technology

45%

of companies surveyed suffered a compromise in the past 12 months.

Source: www.techtarget.com

Safe Social Networking

Sites such as LinkedIn are increasingly used to target employees. A Check Point Research (CPR) report found that in Q1 2022, social networks were the most likely to be imitated to steal data. Also, the report found that LinkedIn was associated with 52% of all phishing-related attacks globally. When assessing your cyber security awareness, make sure to include the following:

- Social phishing types: what tricks are used on social media to steal information?
- Oversharing: the dangers of putting personal or corporate information on a social media site.
- Malicious social links: how social media links can be dangerous.
- Fake accounts: do employees know how to spot fake accounts that can be used for social engineering purposes?
- Privacy settings: are employees trained on using the most appropriate privacy and security settings in their social media accounts.

Preventative measures:

- Security awareness training
- Security hygiene
- Social media security policies
- DNS filtering

69%

have deleted or thought of deleting a social media account because of recent social media data breaches.

GET IN TOUCH