The 2022 Guide to Reducing Human Cyber Risk

Learn how to boost your organisation's employee security posture against human error and evolving cyber threats.

Transforming humans from the 'weakest link'....

Employees have long been viewed as the 'weakest link' in a business's cyber security chain and, with human error still being the number one cause of data breaches, that unwanted crown has rightly been fixed for quite some time.

Even with organisations allocating more time and money towards tackling human cyber risk, employee-related security incidents continued to plague businesses in 2021. But why was that?

Simply put, many businesses just aren't doing enough to combat evolving threats. With cybercriminals using more advanced techniques to exploit humans, the traditional route of once-per-year security awareness training just isn't enough to protect today's businesses from the loss of sensitive information, reputational damage and financial repercussions.

11s

Estimates suggest that in 2021 a cyber attack took place every 11 seconds.

$6T

Cyber attacks were projected to hit $6 trillion in annual losses in 2021, which has doubled since 2015.

200

The average business cost of a cyber attack is $3.86 million and breaches take over 200 days to be detected.

...into a cyber security asset.

Good news is, the solution to user-focused security has also evolved in recent years through the introduction of Human Risk Management (HRM), offering a much more robust level of protection for businesses of all sizes and sectors. In this guide, will cover why employees create an insider threat and how to drive secure human behaviour in your business.

Humans — The #1 cause of cyber security breaches

85% of data breaches involve the human element

Verizon 2021 Data Breach Investigations Report

Negligent employees cause about 62% of security incidents

60% of organisations have more than 20 incidents of insider attacks in a year

82% of IT leaders see a greater risk of insider threats if their company adopts a permanent hybrid working structure

98% of organisations say they feel some degree of vulnerability to insider threats

What are the main types of insider threats?

Negligent insiders

Negligent insiders - e.g. an employee who misdirects an email or accidentally attaches the wrong file - are the most common threat to your business and account for 62% of all security incidents.

Negligent insiders who have their credentials stolen

Negligent insiders with stolen credentials - e.g. an employee whose username and password are exposed on the dark web - account for 25% of all security incidents.

Malicious insiders

Malicious insiders — e.g. employees or ex-employees with malicious motivations towards the business, such a as a disgruntled employee who was recently fired — account for 13% of incidents.

Why are employees an insider threat?

1

Humans make mistakes

We all make mistakes. In fact, 43% of employees say they've made a mistake at work that compromised cyber security, such as misdirecting an email. Problem is, these types of 'small' mistakes can result in sensitive data being exposed, which attackers are experts in exploiting.

88%

Stanford University attributes 88% of data breaches to human error, even more than Verizon.

43% of employees say they've made a mistake at work that compromised security.

2

Humans are targets

Much of your business's information can be found online, including your suppliers, contractors, and customers. This makes it easy for attackers to impersonate internal and external contacts, and all it takes is for one person to be successfully duped for your business to be at risk of a serious breach.

In 2021, phishing attacks were connected to 36% of breaches, an increase of 11%.

25% of employees believe they have clicked on a phishing email at work.

3

Humans break the rules

People in any business are capable of breaking the rules, be it maliciously or accidentally. But a large portion of rule-breaking ventures further than not abiding by password policies - some employees can go as far as to steal corporate data and sell this on the dark web.

45%

of employees would be willing to sell corporate info to people outside their organisation.

70%

of malicious insider breaches are financially motivated, mainly by selling credentials on the dark web.

4 key causes of a user-related data breach

Human error

An employee mistake, such as a simple typo, can seem small... but the repercussions can be huge. For many businesses, a human error-related breach has resulted in fines, loss of customer trust and losing access to data.

Common ways that risky employee behaviour can lead to a security incident

- Sharing, writing down or re-using passwords across multiple accounts
- Carelessly handling data, like entering the wrong email recipient or attaching the wrong file
- Lacking awareness of common threats, such as spear phishing emails
- Failing to understand that security is the responsibility of all employees, not just a problem for the IT department

Employee falling for a phishing attack

The most common way of an employee causing a security breach is by falling for a phishing attack.

And with phishing being more targeted and sophisticated than ever before, employees are finding it increasingly difficult to spot these attacks.

The clever techniques attackers use to reel in your employees

- **Spear Phishing —** These hyper-personalised attacks target a specific individual or group, with the attacker conducting prior research into an often senior-level target.
- **Business Email Compromise —** If an attacker gains access to a legitimate email account, they can exploit 'colleagues' by posing as a trusted source via a BEC attack.
- **Domain Spoofing —** An attacker can fake the display name and sender address of an email to make it look like it came from inside the company or via a trusted vendor.

Employee mishandling credentials

Employee password behaviour plays a huge part in security incidents, with 61% of breaches involving stolen credentials, costing businesses $4.37M (US) on average.

By re-using the same password across multiple accounts, one third-party breach can create a portal of human risk for your business.

The road to compromised credentials

1. Employee signs up for multiple third-party services using the same business email and password.
2. A third-party service suffers a data breach, exposing the user's credentials.
3. The credentials are sold on the dark web, which attackers can potentially use to gain access to multiple accounts.

Inside the Dark Web

- The Dark Web is 500x larger than the surface web.
- Dark web activity has increased by 300% since 2017.
- More than 22 billion records were added to the dark web in 2020.
- 60% of the information available on the dark web could potentially harm enterprises.

A lack of security policies and processes

Information security policies help guide employee behaviour when it comes to handling company information and keeping IT systems secure.

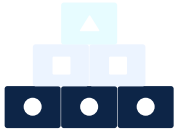
Without these policies, employees are less likely to know who they should be reporting phishing attacks to or who is allowed access to which sensitive data.

How can policies help reduce risk?

- They protect your organisation's critical information by clearly outlining employee security responsibilities.
- They prevent unauthorised disclosure, disruption, loss, access, use, or modification of an organisation's information assets.

Good policy examples

- Acceptable Use Policy
- Confidential Data Policy
- Email Policy
- Incident Response Policy
- Network Security Policy
- Password Policy
- Physical Security Policy



Establish a security-minded culture — The foundations

A 'security culture' aims to encourage all employees to think about and approach security through the same values, encouraging people to follow the desired behaviours that will keep staff, customers and suppliers safe. Building this culture requires a number of factors, including consistency, time and effort. Here are some of the key building blocks to creating a security-savvy workforce.

Get support from the top

Executive support is crucial for the success of any human risk management initiative. We don't just mean a send-to-all email from the CEO - we mean the leadership team demonstrating their full support for this initiative through regular communications to staff, assigning the necessary budget and creating specific business roles.

Consistency and commitment is key

The key to building and maintaining a security-savvy workforce comes in the form of consistent and long-term user training, as pointed out in a report by Keepnet Labs, where consistent security awareness training was proven to reduce employee phishing susceptibility from 60% all the way down to 10% within the first 12 months.

Time, not budget, is the blocker to beat

According to the SANS 2021 'Managing Human Cyber Risk' report, 75% of security professionals spend less than half their time on security awareness, even though more dedication to training correlated with an increase in positive behaviour change.

Treat security as everyone's responsibility

Employees need to understand that cyber security is the responsibility of every employee, not just the IT department. Employees are given more access to computers and online resources than ever before and are widely seen as a business's biggest risk. It's important that people know the importance of working together to ultimately achieve cyber security.

Go beyond security awareness training

Security awareness training is a great way to reduce human cyber risk, with 80% of organisations seeing a reduction in phishing vulnerability when training staff. But in order to truly build a resilient workforce against evolving threats, policies must be implemented and practical assessments, like phishing simulations, must regularly take place.

Strategic alignment is crucial

SANS also report that leaders must make long-term, strategic investments in people, just as they would for other security efforts like vulnerability management, incident response or security operations centers, in order to effectively manage human risk.

Implement Human Risk Management (HRM) — The fundamentals

Human Risk Management (HRM) enables businesses to assess, reduce and monitor their ongoing employee security posture against evolving cyber threats and human error. With these threats becoming more complex and sophisticated, HRM delivers a fully-rounded solution for driving secure human behaviour, rather than relying solely on user training in the hope that something sticks. There are four key elements to HRM:

Drive secure user behaviour

Security awareness training is one of the most effective approaches for reducing human cyber risk, with businesses expecting to see an ROI of between 69-562% (Osterman Research).

Delivered via computer-based training, these sessions should be regular, short and cover a variety of core information security and compliance topics.

Improve security processes

Implementing a **policy management** process helps staff understand and act on their responsibilities, boosting the protection of business information and IT systems.

Policies should address a number of key areas (see examples on the next page) and should be updated and signed by staff at least annually to keep processes fresh.

Reduce phishing vulnerability

Not only do **phishing simulations** allow businesses to assess human vulnerability to common attacks, but they also offer the chance to reinforce user training and measure each user's progress.

Ideally, simulations should be conducted quarterly in order to test new and trending attacks, whilst assessing the risk level of new employees.

Mitigate external threats

With millions of usernames, passwords and payment details being dumped onto the dark web each year, ongoing **dark web monitoring** alerts businesses when employee data is found to be compromised.

Catching these early threats can ultimately prevent a targeted attack - and potential data breach - later down the line.

Cover the essentials to maximise success — The best practices

9 tips for tackling long-term human risk

Learn what the key ingredients are for a successful Human Risk Management approach.

- **Make training short & engaging —** Use short video training courses to engage staff
- **Cover the essentials —** Be sure to cover key security topics (see these further below)
- **Train staff regularly —** Monthly training keeps knowledge fresh in the mind
- **Avoid technical jargon —** Many employees won't understand industry terms
- **Replicate common phishing threats —** Test staff against scams they're likely to face
- **Deploy quarterly phishing simulations —** This helps monitor risk without overkill
- **Cover core policies —** Make sure your policy library includes the essentials (see below)
- **Keep policies up-to-date —** Review and update policies each year
- **Measure the impact —** Track training performance and simulations over time

Key training topics for your staff

- Phishing Attacks
- Passwords & Authentication
- Working Securely from Home
- Secure Internet & Email Use
- Physical Security
- Social Engineering
- Mobile Device Security
- Public Wi-Fi

Common phishing scams to test on your workforce

- New Microsoft Teams request
- Coronavirus advisory alert warning
- Office 365 password expiration
- Deactivation of old OneDrive account
- OneDrive shared contact notification
- Starbucks bonus
- WHO coronavirus safety information
- New voicemail message alert

Essential security policies to implement in your business

- Acceptable Use Policy
- Confidential Data Policy
- Email Policy
- Mobile Device Policy
- Incident Response Policy
- Network Security Policy
- Password Policy
- Physical Security Policy