eBook

7 Reasons Why Humans Will Cause you a Data Breach



Enso Solutions

Table of Contents

Introduction (Page 1)

Reason no. 1: “They use weak and reused passwords” (Page 3)

Reason no. 2: “They send sensitive information to the wrong recipient” (Page 5)

Reason no. 3: “They click on links in emails” (Page 7)

Reason no. 4: “They intentionally steal data for financial gain” (Page 9)

Reason no. 5: “They misplace stuff or leave it unlocked” (Page 11)

Reason no. 6: “They easily believe what others say” (Page 13)

Reason no. 7: “They openly talk with others about sensitive company information” (Page 15)

Conclusion (Page 17)

Introduction

The human factor is the biggest reason businesses face data breaches, according to analysis of data from the UK Information Commissioner's Office (ICO) 90% of all breaches in 2020 were caused by human error. Clicking on links, misplacing data and equipment, giving way sensitive company information, and weak passwords have all contributed to the hundreds of thousands of incidents and breaches in the last 12 months.

Even with increases in cybersecurity budgets of detailed and advanced cybersecurity strategies over the last 10 year's, businesses are still being impacted by breached. It will also be impossible to fully secure the business, its assets, and data without help from humans, your employees. And in many cases, employees are more of a threat than any hacker could dream of being.

Human error is happening all the time, whether it’s an email delivered to the wrong person, staff inadverently clicking on an unkown link, an IT admin that hasn’t installed the latest Windows OS patch, or even an employee divulging too much company information to others outside of the business. Human error will occur when there is an opportunity for it to do so. We must look to eliminate the opportunities as much as we can.

In this eBook, we will look at 7 reasons humans are a huge security risk to your business, and what we can do to mitigate these risks.



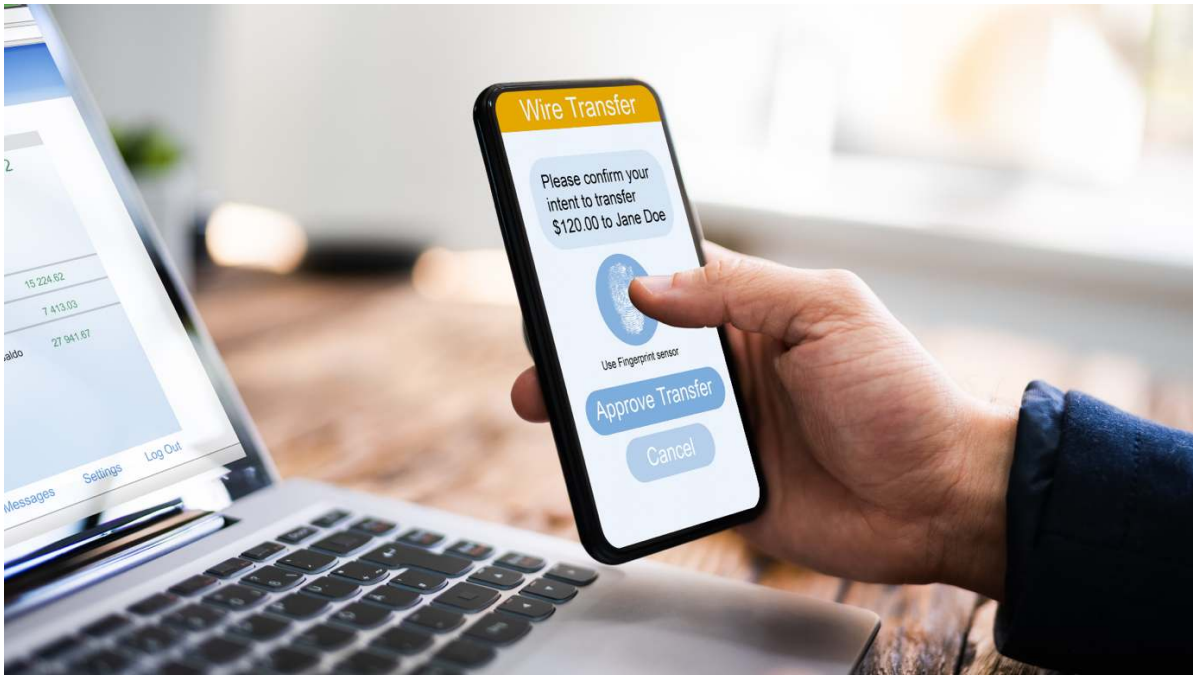
Reason no. 1: “They use weak and reused passwords”

Cyberattacks are happening more frequently, and getting more complex in nature, but still, a common cause of a data breach is due to either weak or compromised passwords, a vulnerability that makes a hacker's job much easier to exploit and gain access to business accounts and data.

Cybersecurity threats keep evolving, but many businesses are still relying on passwords as an effective security control, which could lead to an expensive data breach. The biggest problem as indentified in a recent survey by Google is that is that 65% of employees reuse the same passwords, and not only for work purposes but for their personal accounts too. If a cybercriminal can steal credentials to just one of these accounts, they can then gain access to all others that are using the same password.

Relying only on passwords in a data loss prevention strategy is risky business. Let's take a look at some more statistics:

- At least 65% of us reuse passwords across multiple websites.
- 13% of us use the same password for absolutely all logins.
- Around 80% of data breaches are caused by passwords being compromised.
- 81% of hacking related breaches are caused by compromised passwords.
- Nearly 50% of us only add a digit or special character when we change our password.



Solution:

Multi-factor Authentication (MFA) should be the default standard for securing login into applications, online accounts, or VPNs, MFA requires the user to provide multiple verification factors and forms part of your identity and access management (IAM) controls. Rather than just standard username and password, multi-factor adds additional layers of security, such as a unique fingerprint of the device being used to logon and one-time passwords. This decreases the likelihood of a cyberattack, since having your username and password will not be enough to logon. This enhances your businesses' security posture and keeps you safe against attacks.



Reason no. 2: “They send sensitive information to the wrong recipient”

Social engineering attacks dominate the headlines, phishing, ransomware, and brute-force attacks tend to be the most common of cyberattacks. However, misdirected emails (that's emails that have been sent to the wrong recipient) are a much bigger problem for businesses. Statistics show that a business with 1000 employees, at least 800 emails a year are sent to the wrong recipient. That’s over 2 per day, every day.

Email addresses are considered personally identifiable information (PII) and are therefore protected under GDPR. Big fines, loss of clients, and damage to a company's reputation, potentially revealing confidential data, and breaching client's privacy, just by sending an email to the wrong Alice or Bob.

With email still the preferred way that we communicate with others, and around 4 billion people use email regularly, sending around 300 billion emails every day. Misdirected email really is a huge global problem that can lead to financial losses, and cost employees' jobs. The biggest reason for misdirected emails is down to the sender being tired, with technical issues being the second.



Solution:

Best practice would be to double-check all email addresses before sending, go through the list of names and email addresses. You could clean up the auto-complete list. Setting auto delays for sending emails could also benefit you, this would then give you a chance to review the outbox before the emails have been sent.

Both solutions above, however, still rely on user intervention. A technical solution that uses AI and machine learning is a better option to ensure emails reach the right recipient. Using past relationships, behavioural analysis and other technologies identify first-time contacts, stopping misdirected emails with sensitive data leaving the business.



Reason no. 3: “They click on links in emails”

Social engineering attacks and particularly phishing attacks are becoming more sophisticated and democratic. It's getting easier to craft legitimate emails that look like they are coming from the government, HSBC bank, or Google for instance. The tools that are available for cybercriminals allow for easily adding a logo, copying and pasting text, and then just add a fake malicious link. With the previous 12 months and a pandemic to deal with, cybercriminals have taken this opportunity to manipulate human nature and emotions. Using human fear to create a sense of urgency, or curiosity.

Don’t get me wrong, there have always been problems with humans clicking on malicious links, but when those humans are working from their home environment, stress, and economic conditions provide the perfect playground for bad actors.

Out of every 99 emails received, one is a phishing scam. If we put this in perspective, every employee in your business receives almost 5 of those phishing emails every working week. Unfortunately, relying on email programs to filter out these messages, is a risky move indeed. It just takes one user to click on a link, and then their user credentials are compromised, or malware is downloaded onto the device, which can then worm itself onto the network, infecting critical business systems and even encrypting data.



Solution:

There are several preventative controls that can be implemented to protect against business email compromise, such as email protection applications providing detection of VIP spoofing, brand forgery and sanitisation of embedded links.

Cybersecurity awareness training, even though training will certainly benefit them don't just rely on users to mitif=gate against these threats alone. Also don't rely on your threat intelligence sources either, with the number of attacks that happen on a daily basis, a new threat could slip through the net. One of the most effective appraches is isolation. All web traffic should be retrieved and executed in a safe and isolated 'Sandboxed' environment.



Reason no. 4: “They intentionally steal data for financial gain”

While not quite human error, it certainly is down to human judgment. Human error implies that a human has made an error or mistake. However, insider misuse is more of a deliberate attempt to cause havoc with business systems, and in most cases, it’s a deliberate use of resources by an authorised user for financial gain and equates to 40% of incidents.

Insider misuse is one of the hardest threats to detect since the bad actor here is someone that the business has placed trust in. Employees have all sorts of privileges, access to servers, databases, hardware, etc.

In almost all cases of insider misuse, the abuse has only been found after forensically examining devices after the human has left the business. The information that has been leaked could have been released months, or even years before the business discovers it.



Solution:

Preventing insider threats can be very difficult, you can, however, limit the damage through security controls by compartmentalisation of the data on your network or in the cloud and adopting a least privileged approach where users are assigned enough rights to complete their job role. The fewer files, applications, and systems a user can access, the more difficult it would be for them to abuse their access, limit access to only data and systems that they require for their day-to-day job. Making sure to revoke remote access as soon as an employee leaves.

Another method would be to monitor employee's activities for suspicious behaviour. Set-up systems for continually monitoring activities of employees, especially around financial, medical, or personally identifiable information (PII).



Reason no. 5: “They misplace stuff or leave it unlocked”

We have a tendency to think about data breaches being a result of some kind of cyberattack, but in reality, a significant number of incidents don’t even involve technology. Statistics show that most physical incidents involve device theft (laptops, storage drives, smartphones, hard drives) and theft of paperwork. With employees working from home, or on a hybrid working basis, keeping an eye on assets becomes increasingly harder, and easier to misplace. An opportunist criminal could easily get their hands on sensitive data.

You wouldn't leave your house or car unlocked overnight, would you? But when it comes to securing our computing environment, it's a differnt matter. Humans are just more careless with their devices than anything else of value in their lives. Pre-pandemic, when we could actually travel, use public transport, or take a taxi home after a night out, a laptop was stolen every 53 seconds, and during the lifetime of the laptop, you had a 1/10 chance that it would be stolen at some point.



Solution:

Firstly, all devices given or used by employees should be controlled by either Mobile Device Management (MDM) or Mobile Application Management (MAM) software. POlicies such as encryption or drives, implementation of timed screen locks, and the ability to remotely wipe the device of business data in event of loss or theft need to be implemented. Think what the worst-case scenario is, if the device were to get into the wrong hands.

Limit the amount of paper that employees can access, where possible, move to a digital environment, where it is easier to secure and manage access. Train employees on best practices, ensure they lock their screens when they move away from devices and secure devices at the end of each day. Reinforce this with communication and acceptance from staff with your Acceptance Use, BYOD, and Remote Working policies, it's critical that they reflect your current working practices so if you haven't reviewed them in the last 12 months update them prior to reaffirmation by your staff.



Reason no. 6: “They easily believe what others say”

Humans are intrinsically gullible. We have a unique ability to trust others and act on stories that we hear. You could say that trusting others is second nature. Unfortunately, not everything we hear from other humans is useful or true. From a cybersecurity standpoint, research has found that almost 25% of data breaches are caused by cybercriminals pretending to be someone that they are not.

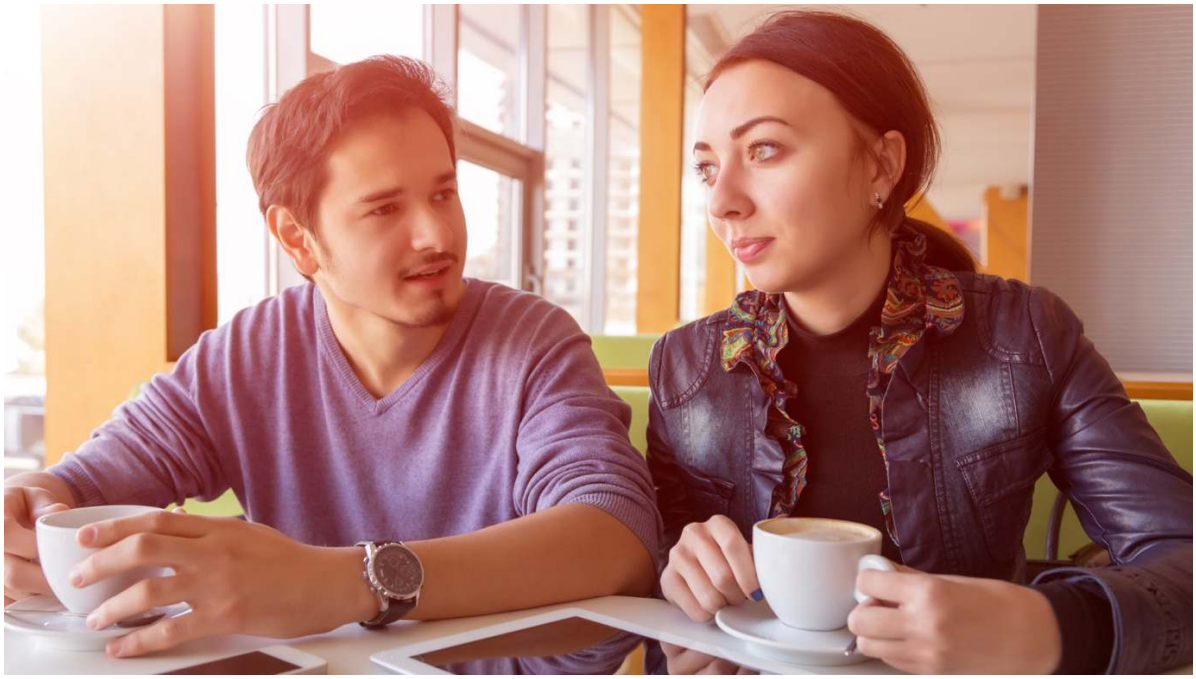
You've heard of phishing, as we have discussed earlier on in this eBook, but what about financial pretexting? Pretexting is similar to phishing in that cybercriminals are looking to exploit humans' gullibility to gain their information (financial information) specifically.

Normally, pretexters contact users by phone or email, and instead of creating a false pretty looking fake website, they simply act like someone else potentially from within the target's own business or from a trusted third party, they request that their target send them financial details, bank account details, etc. Once this information has been received, the cybercriminals can then commit fraud, or sell their data or contact a third party, this data could be used to contact the victim's bank or a supplier to request additional account history



Solution:

You can reduce these pretexting scams, by email filtering and access to out-of-policy applications with insider threat management tools. Awareness training is also a good idea and is key to help employees understand the associated risks of pretexting scams, how information should be handled and to stay alert, and how to report incidents if they believe they have encountered a scam.



Reason no. 7: “They openly talk with others about sensitive company information”

We have heard 6 reasons why humans will cause you a data breach in 2021, we have one more left.

You may have heard the saying, 'Loose lips sink ships' which dates back to World War 2 when spies were all around us, and this is the reason for number 7. Similar in nature to reason 6, instead here we are talking about humans need to talk about things that they shouldn't, especially outside of the office environment. Even idle gossip can lead to a data breach.

Employees are exposing themselves and the business to cyberattacks, and damage to company reputation when they openly discuss business affairs out in the open. Which could then lead onto to pretexting or phishing attacks, which can have a higher success rate due to knowing sensitive internal information which should be only known by employees working inside of the organisation.

Solution:

Policies and awareness training are the only way to prevent this from happening, as there are currently no known technical solutions that can be used to quieten an employee when outside of the office environment.



Conclusion

Humans are integral to cybersecurity. We are the target – the solution – and the problem. As we have heard throughout this eBook, the root cause of most cybersecurity breaches is human behaviour. So, while focusing on external threats is a good thing, we cannot dismiss this critical and weakest of links, our employees.

Many cyberattacks are designed to bypass security controls and simply exploit human error. Social engineering attacks and particularly phishing attacks, deceive humans into thinking that the attacker is coming from a trustworthy source, it only takes one employee to click on a malicious email for malware to be installed across critical business systems. These attacks can be difficult to defend against and become even more challenging with remote based workforces, who often use their own personal devices to connect to the network

How can businesses protect against the human threat?

Businesses shouldn’t overly focus on technical controls, it's important but so are their most important assets: their people. Without addressing the human element, Businesses become vulnerable.

Here are some steps that should be taken:

- Implement strong and robust training and cybersecurity awareness programs
- Implement plans to identify and deal with fraudulent behaviour
- Be aware of the risks posed to the company and personally owned devices
- Learn how to safely dispose of personal information and teach others how to do so
- Use encryption where possible

Businesses should encourage employees to report potential security breaches, incidents, or scams without being in fear of repercussions. Security leaders should lead by example and create an environment where security is seen as a shared responsibility, communicating to employees that they are key in safeguarding against cyberattacks.

About Enso Solutions

We're an agile, proactive and experienced provider of business enabling Network, Security and Connectivity solutions backed by passionate people and leading partners. We are focused on assessing, designing, delivering and managing core technology solutions in partnership, empowering you as decision makers. Helping you to create value, protect your business and accelerate change in today's rapidly evolving digital world. We specialise in leveraging our experience in supporting our "Small to Mid-sized" enterprise customers on their journey through digital transformation and secure workforce mobility.

CONTACT US

e: info@ensosolutions.com

t: +44 1534 662 662

w: www.wepreventdatabreaches.com