+44 345 094 0945
www.waterstons.com
Article

Cyber mistakes: past, present and future

Dec 2023

Cyber mistakes: past, present and future

Can Scrooge learn from his mistakes and create a cyber security culture?

Categories Cyber Resilience, Cyber Security Strategy, Cyber Essentials and ISO 27001

Dec 2023

Rhianne Short

Information Security Consultant

Email

rhianne.short@waterstons.com

Cyber security was ignored, to begin with. There is no doubt about that, Mr Scrooge rebuffed the threats, mocked the scaremongers and signed in to unprotected devices without a care.

He was ferocious in his business dealings; some would say a tight-fisted hand at the grindstone. Password managers or anti-virus software had no influence on him – he was intent upon growing his business tenfold, and not letting anyone – or anything – get in his way.

One Christmas night, his trusty CISO, Bob Cratchit, approached Scrooge with trepidation.

“Excuse me, sir” he said, “but tomorrow is Christmas Eve, and with the office shutting over the festive break, we really should implement cyber security measures to protect the business, our funds, and the data of our team and clients.”

“Humbug,” exclaimed Scrooge grumpily. “A poor excuse for picking a man’s pocket. We have nothing to fear.”

With that, Scrooge gathered up his things and went to the pub - it had free Wi-Fi so he could login to company systems without a care, USB charging points at the tables for his work phone, and the food was cheap.

Full of sausage and mash, with client data cleansed and some finances corrected, Scrooge headed home. His Ring doorbell seemed strange that night – as if it were moving independently. Putting it down to too many drinks, he once again cursed the incorrect QR codes meaning he had to keep getting up from the table to get to the bar, he heads inside.

It was strange when Bob Cratchit’s face came to him as he slept, even stranger when, in his dream, he told him he needed to learn some cyber security lessons and would be visited this very night to do just that. Scrooge didn’t heed Cratchit’s warnings while waking, so why should he when asleep? If only he knew.

The mistakes of cyber security past

With a blast of cold air, Scrooge awoke with a start. Infront of him was his first business mentor; a young man no older than he, who could only talk about data protection and creating a cyber security culture from the start, whatever that means.

“I warned you,” scolded the young man. “A security culture is more important than you think.”

Scrooge learned that a security culture is the collective mindset and behaviours within an organisation that prioritise protecting sensitive information and technology from cyber threats. It involves being aware of potential risks, following security practices, reporting potential incidents, and fostering a shared responsibility to ensure a secure cyber landscape.

Measuring something as subjective as the strength of security culture in an organisation can be difficult, and sometimes there may be a general sense of how strong it is, but measuring using other means, in order to create a security baseline, manage any associated gaps and risks, track its progress and improve it over time is more important.

The mentor explained one way of measuring the strength of the organisation’s security culture is through employee surveys and feedback; a great way of getting direct insights into the day to day understanding, and perceptions of cyber across the business.

This could be complemented by a more objective measurement, such as using security assessments and audits. Many security standards or frameworks, such as Cyber Essentials, often look at security awareness and culture as part of their analysis, providing a more unbiased evaluation of the security culture, and offer actionable insights to enhance the culture.

Benchmarking is also a crucial element in measuring security culture to allow comparison against industry standards and best practices which help identify areas for improvement and continuously enhance an organisation’s security posture.

Benchmarking can be done by utilising data collected from training providers or security organisations, utilising the Department for Science, Innovation and Technology Cyber Security Breaches Survey, and speaking to other organisations about cyber security and their successes and challenges within networks and forums.

“You must learn from others,” the mentor warned, fading into the darkness. “You cannot do this alone.”

The mistakes of cyber security present

No sooner had he fallen back into slumber, Scrooge once again woke to find another figure in his room – this time, it was a man he’d seen many times in the pub after work, but never met.

“What are *you* doing here?” enquired Scrooge, put out not only for yet another unexpected guest, but for having his sleep interrupted once again.

“I’m the ghost of your present cyber security mistakes,” he answered, “and trust me there are many we need to discuss.”

With the click of a finger, Scrooge and the mysterious figure were transported back into the pub from that very evening. Sitting at a table was Scrooge, tucking into his meal and periodically leaving his laptop to return to the bar, visit the loo, or berate a member of staff for some minor inconvenience.

Around him were people engaging in festive cheer. Women in sequins were drinking brightly coloured cocktails, men wore novelty ties with flashing lights. All were singing along to the music, making toasts and donning hats from crackers. To Scrooge’s mind, the worst type of frivolity.

“What is wrong with this scene?” asked the stranger who had taken him back to this place. Many things, thought Scrooge, but nothing that he was involved in.

Working from anywhere can be unavoidable, but it means more threats and security issues, and things to be aware of.

Leaving laptops unlocked and unattended, potentially allowing unauthorised access to sensitive information, can be a significant security risk, potentially leading to data breaches or social engineering attacks. Devices should always be secured and in possession to safeguard both personal and company data.

Being aware of the type of data being accessed when working in a public area, limiting access to confidential information to avoid ‘shoulder surfers’, and observing the tasks being worked on is vital to reduce the risk of confidential information being exposed.

Using USB charging points when working in a public area can also pose a security risk as malicious actors can exploit these connections to transfer malware or gain unauthorised access to a device, potentially compromising sensitive information. It's important to stick to trusted charging sources and avoid public USB ports to prevent potential security breaches.

Using free public Wi-Fi is another risk that could expose a device to potential security threats, as these networks are often unsecured, making it easier for cybercriminals to intercept sensitive data such as login credentials. If using free public Wi-Fi is unavoidable, use a virtual private network (VPN) or avoid accessing sensitive accounts and data while connected to public networks.

The stranger disappeared in a flash, leaving Scrooge to wonder on what he had just been told.

The mistakes of cyber security future

Unable to resume his slumber, Scrooge sat upright in bed, awaiting his third, and hopefully final, visitor. It wasn’t long until he felt a cold shudder and knew they had arrived.

A tall, silent man wearing a very smart suit stood in front of him, and beckoned Scrooge to follow.

Where he took him was worse than anything he’d seen so far that night, for they visited Scrooge’s office. But it wasn’t his name above the door, or his team with their outdated laptops. This place was modern, the staff looked happy, and he noticed many locked screens – surely that drove down efficiency through wasted time entering passwords?

“What has become of my business?” implored Scrooge of his smartly-dressed guide.

“This is not your business,” he replied, emotionless. “Your data was compromised as your team were not trained to look for security threats. You were hacked, all your assets lost, and all data leaked.

“I am the case investigator and found you wholly negligent to your responsibilities. This is the firm that moved in, took all your clients and built an empire on your rubble, doing everything you didn’t.”

“But, what became of me?” asked Scrooge timidly, unsure if he wanted to know the answer.

“You were banned from ever owning or running a business again. You now live in a bedsit in Crewe and work at ASDA.”

It was too much for Scrooge. He tugged at the man’s lapels and begged his forgiveness, promising to do better. But it was in vain. What he was grasping was his duvet, and he was waking – for the final time – to Christmas Eve sunshine peeking through the gap in his blackout curtain.

He needed to make a change; not only of his attitude towards technology, but also to protect his team and his business.

He sprung out of bed, quickly got ready and bounded into the office before any of his team arrived. By the time they got there, he had a plan: He was going to create a cyber security culture.

He plans to create and continually improve this through:

- **Education and training of employees –**the benefits of the training should be highlighted to staff, being clear about how the training will help not only them, but also the organisation as a whole.
- Creating **awareness campaigns -** Such as having a regular monthly or weekly cyber security article in your staff newsletter, writing blog posts, a senior manager sending out an email with cyber security tips, advice and reminders, hosting internal events or webinars about cyber, having physical reminders in offices through posters or using digital screens, using awareness days as a hook for positive cyber messaging, and talking about cyber in meetings and other forums used within your organisation.
- **Drills and simulations** that include phishing simulations for staff to see who may be clicking on potential phishing emails, monitoring the reporting rates of phishing simulations, incident response rehearsals, and physical security social engineering testing at your offices and organisation buildings.
- **Incentives and recognition** for positive cyber behaviours. This can be done in a number of ways, such as getting teams to compete to see which teams can get the highest compliance rate on their training, and giving a prize to those teams that

do, having a cyber champions scheme and giving rewards and prizes to staff that have demonstrated good cyber behaviours.
- **Open dialogue and continual feedback**. If staff have a fear of getting into trouble when clicking on a possible phishing link, they are going to be a lot more likely to try and hide it than report it. Fostering a no blame culture creates more trust and transparency, which often leads to incidents being reported a lot quicker, which can lessen the impact and improve your overall security.

By the following Christmas, Scrooge had devoured the NCSC website for helpful advice, run regular training activities for his team, included cyber security in all on-boarding activity, and even started the process of getting the Cyber Essentials accreditation.

In changing his attitude, Scrooge changed his business for the better, and massively reduced the risk to it.

We all learn from mistakes, we just hope you aren’t visited by visions of them in your sleep.