Crowe

Six Steps To Better Cyber Hygiene – Expert Tips

Balancing technology, people and planning is crucial to a successful strategy, according to Cyber Risk Aware CEO Stephen Burke

Worldwide spending on information security was predicted by global research and advisory firm Gartner to grow to US$123.8 billion in 2020. But with cybercrime on the rise – an increase that has been greatly amplified by the coronavirus crisis in large part thanks to the switch to mass home working and a greater use of personal devices – organizations around the world are still set to lose trillions.

If these enormous numbers reveal anything, it's that investment in technology is far from a panacea for tackling cybercrime. Instead, a holistic approach that balances the roles of technology, people, and planning, while identifying and addressing the flaws in each, is the best way to minimize risks, reduce security vulnerabilities, and prepare effectively for potential cyberattacks and data breaches.

Cybersecurity is an important topic in 2021 for organizations of all sizes. Business leaders must be bold. They have to make smarter decisions both in terms of investing in innovative technology solutions and installing processes that protect internal data as well as customer data and accommodate digital growth.

Most companies could – and should – improve their cyber hygiene, and that comes from the top down. Consider that human error caused 90 percent of UK cyber data breaches in 2019, according to cybersecurity analysts CybSafe – and it's a similar picture globally.

Stephen Burke, Founder and Chief Executive Officer of Cyber Risk Aware, a security awareness training company based in Ireland, tells Crowe that business leaders who want to make smarter decisions around cybersecurity must realize there's far more to consider than just the latest technology or maintaining a robust IT department. In fact, a company's culture and attitude to cybersecurity actually matter the most.

Exclusively for The Art of Smart, Mr Burke identifies six key steps to establishing an effective and inclusive cybersecurity program.

1. Identify the relevant risks

Cybersecurity risks are commonly linked to an organization's key assets. "With limited time, people, resources and money, there's only so much you can focus on," acknowledges Mr Burke. "Not all risks are relevant to every business; it's about identifying what risks are key and material to you that need to be addressed."

2. Engage the whole organization

Establishing an IT steering committee that encompasses a core section of the business at a senior level, while identifying the risks associated with systems or data in each department, will improve cybersecurity.

"You have to bring the whole company along – you can't do it by yourself," explains Mr Burke. "Bring people along in a meaningful way, tied to the risks, using the language of the business, and register what the company needs to worry about."

3. Evaluate the effectiveness of existing controls

“When you apply a control, which might be a technical control, a process, or people, it brings [the risk] down to a residual level,” says Mr Burke. As such, it’s important to pinpoint existing controls and measure how effective they are.

He continues: “That then informs what we need to invest in to bring the level of risk down, so that the company can say: ‘Look, this is what we did, we saw this risk, we applied these controls and we’re happy with the level we’re getting to.’”

“Bring people along in a meaningful way, tied to the risks, using the language of the business, and register what the company needs to worry about.” - **Stephen Burke**

4. Address the human factor – education raises awareness

What’s often missed is how important it is to invest your people, and not just those working in the IT department. Educating all staff members about how to improve cyber hygiene and establishing protocols should data breaches occur are vital activities.

“You have to assess where the vulnerabilities are in your staff, so a human cybersecurity awareness program would be a key step,” explains Mr Burke. “[These programs] assess where the gaps are with staff knowledge, assess the susceptibility of phishing emails, and target training to those individuals who need help.”

5. Find and strengthen your technical weaknesses

If you can catch technical difficulties and tackle them accordingly, you’re addressing a larger part of the problem.

“One of the major threats today is around credential harvesting: that is stealing people’s usernames and passwords,” says Mr Burke. “They’re for sale and therefore a lot of cybercriminals have access to pretty much every password. But if you turn on multi-factor authentication, you will secure 99 percent of the credential harvesting.”

6. Formulate a plan and test it

Businesses should prepare for the possibility of cyberattacks with an incident response plan – this has both practical and legal benefits, and it is here that smarter decision-making can be achieved. An incident response plan involves identifying who is going to make decisions on behalf of the organization in the event of a security breach. The plan also needs to outline how staff members will communicate if corporate systems are down, as well as address things like the legal, ethical and moral questions around paying ransoms.

Mr Burke comments: "President Dwight D. Eisenhower said: 'Plans are useless, but planning is indispensable.' What he means is you have to test the plan. If you're not running regular tabletop exercises of your plan, you're not going to find where the gaps are." Failure to plug them could prove costly to your organization, both financially and in terms of reputation.

How To Think Like A Cybercriminal

It's critically important to know your enemy, and work out what vulnerabilities your business might have, says Jim Gee of Crowe UK

Crowe has a unique approach to cybercrime protection: it steps into the shoes of the cybercriminal, uses similar techniques to online offenders, and goes undercover on the dark web. Given that a July 2019 Crowe report calculated that fraud is likely to cost individuals and businesses US$5.1 trillion a year – with losses rising by 56 percent in the past decade – it is potentially more costly to not use all available ways to combat this significant threat.

"We perform an external vulnerability review, which looks at the vulnerabilities cybercriminals could see in an organization if they wanted to investigate whether they should spend time attacking it rather than another business," explains Jim Gee, National Head of Forensic Services, Crowe UK.

Alongside the external analysis, Crowe investigates with an internal vulnerability check. This process is similar to the first stages of a penetration test, or authorized cyberattack, but without exploiting the weaknesses inside the business.

"We've developed identities over the past few years that allow us to go into the markets and forums on the dark web, where most cybercrime and fraud is organized," says Mr Gee. "We can see what's being discussed, we can see what's being sold and that allows us to look for evidence of discussions taking place about attacking particular organizations and for compromised emails and passwords."

Given that cyberattacks rank first among global human-caused risks, according to the World Economic Forum Global Risks Report 2020, and cybercrime may cost US$11.4 million every minute in 2021, it is clearly business-critical for organizations to shore up their defenses.

“COVID-19 has seen a massive surge in cybercrime,” continues Mr Gee. “It is not a question of if an organization will be attacked but when.” For response to be effective organizations must understand the three following things, he suggests.

1. Technology needs to be used to be as well protected as possible but we also need to be ready to manage an attack if it happens and to be able to recover and mitigate any damage – the approach has to be comprehensive.

2. These are cybercrime businesses making business decisions about which organizations are the best to attack in terms of the resource needed and the potential benefits.

3. Cybercrime is not like other phenomena that we seek to manage as risks; it is not static but extremely dynamic, continually changing and evolving like a medical virus. This means that what organisations do to protect themselves also needs to evolve and change to reflect the latest manifestations of the problem.

Viewpoints from Crowe

Nadeem Maniar, Fraud & Forensic Director, Crowe UAE

“Each one of us is either a target or a victim of cybercrime. Human error caused 90 percent of cyber data breaches in the UK in 2019, according to the Information Commissioner’s Office – and it’s a similar picture around the globe. The Middle East’s digital markets have been expanding with an annual growth rate of 12 percent and correspondingly the cost of data breaches is increasing at an alarming rate. In August 2020, The National [a Middle East newspaper] reported that the cost of a data breach in Saudi Arabia and the UAE has risen by 9.4 percent over the past year. These incidents cost companies studied in the region US$6.53 million per breach on average, which is higher than the global average of US$3.86 million per breach. The best defense is a good offense. The right systems and controls, timely awareness, the latest techniques, and an experienced professional partner like Crowe can help you and your organization mitigate the risk of cybercrime.”

Bibliography:
UK Information Commissioner’s Office (ICO), 2019.
Association of Certified Fraud Examiners, 2020. Fraud In The Wake Of COVID-19: Benchmarking Report.
IBM Security, 2020. Cost Of A Data Breach Report.

Geert-Jan Kroll, Technology Advisory Partner, Crowe Peak (Netherlands)

“With organized crime having entered the picture, cybercrime has become one of the world’s largest illegal economies, reaching US$10.5 trillion annually by 2025 – up from US$3 trillion in 2015. The cost of one single incident is often high enough to make companies go out of business in under six months. With technology and automation, cyber criminals need less skill to threaten companies and look for vulnerabilities to exploit. With new techniques and methods emerging daily, the threat landscape changes constantly. This can make it quite difficult to protect your digital assets and company from cybercrime. I think the cybersecurity paradigm should shift from prevention to a more cycle-based approach. This means that companies should apply the ‘assumption of breach’ principle in which they assume that sooner or later they will be struck by a security breach or incident. What companies should do, besides protecting their digitals assets, is to implement measures related to incident detection, response and recovery in order to be able to act accordingly once an incident takes place. Business leaders should adopt the belief that every company is a lucrative target for cybercriminals and that, by practicing good cyber hygiene, they can drastically reduce the risk of becoming a victim of cybercrime. Cybersecurity is about people, processes and technology. In this way, a company’s attitude to cybersecurity and culture matters most.”