Digital Business Ireland

PROTECTING YOUR INFORMATION IN A DIGITAL ERA

A Cyber-Security Guide for SMES

www.digitalbusinessireland.ie

AUTHORS

EJ Wise

Sqd Ldr (ret'd) EJ Wise served for 21 years as a Royal Australian Air Force Legal Officer in a wide variety of key operational roles including counterterrorism, and in locations across the world including Iraq.

Postings included RAAF Headquarters Air Command, No 395 Expeditionary Combat Support Wing, No 462 Cyber and Information Operations Squadron and as an Exchange Officer with the US Air Force at the Pentagon. Today she is a Melbourne based lawyer and one of the world's leading experts in cybersecurity law and the regulatory environment of cyberspace. EJ is Adjunct Professor and Executive Advisory Board member for Cyber at Deakin University, a member of the Royal Melbourne Institute of Technology's Industry Advisory Board for Cyber, and on the Advisory Committee of the University of New South Wales Institute of Cyber Security. EJ is cybersecurity instructor and tutor on the Joint Command & Staff Course at the Irish Defence Forces. EJ can be reached at: wiselaw.com.au

Dinos A. Kerigan-Kyrou

Dinos Kerigan-Kyrou is visiting lecturer in Strategic Cybersecurity at Abertay University. He is a co-author of the NATO / Partnership for Peace Consortium Cybersecurity training programme and curriculum. He is also an instructor on NATO DEEP (Defence Education Enhancement Programme). He is responsible for the cybersecurity training on the Joint Command & Staff Course at the Irish Defence Forces.

"While everyone across the country is focusing on doing their very best during this crisis, there are others that want to take advantage of the pandemic via cyberspace, the online environment in which all of us now live and work. The outrageous attack on the HSE in May 2021 will not be the last time time we face similar challenges in our organisations, companies, and homes."

"Criminals will target both you and your company - faking emails and phone calls, pretending to be from people and organisations you trust. "

"Cyber Security - or Information Security - concerns everyone working across the State. Your own cyber security and that of your organisation are directly linked."

WHAT CAN YOU DO?

PROTECT YOUR EMAIL

Your personal email is the gateway to everything you do online. So it's your number one information security asset. It is therefore critically important to protect, using the following steps:

- Ensure your email password is complex (eg 12 characters long, a mix of letters (upper and lower case), numbers and symbols), and used only for your email. Ensure that it is not a password that is used by you for anything else.

- Use 'two-factor authentication' - 2FA. 2FA is the single most effective mechanism for you to protect yourself online. Easy to set up - it'll take a few minutes but could save you years of loss and stress. Simple 2FA instructions can be found at: www.ncsc.gov.uk/cyberaware/home

ADOPT AN INFORMATION SECURITY POLICY

Commit a draft policy to writing that focuses on how you intend to secure your information and the information of your colleagues and customers.

In fact, a robust information security policy should be continually adapted and improved - but you need to start a draft to protect your information assets. As part of this process, focus on creating an Information Security Management System. Think also about your regulatory requirements, such as the General Data Protection Regulation (GDPR). Consult everyone across your organisation when writing and adapting the policy to ensure their buy-in.

- **Identify Problems Early**

Criminals have an almost infinite number of opportunities to target your company. The only way we can stop them is for every single person in your organisation to be empowered to identify information and cyber security problems as early as possible - regardless of who the person is in your organisation, or what authority they have.

If anyone in your company reports a possible cyber security problem - show your appreciation regardless of whether they have offset a breach or not and regardless of how it was caused. Encourage your staff to spot potential security problems, no matter how they came about.

Look out for when records have been altered, or files accessed or uploaded unexpectedly, or passwords are being shared - these are signs that there may have been a data breach.

Digital Business Ireland

A business culture that encourages collaboration and early identification of security challenges is critical for ensuring robust cyber and information security.

A business environment that forces employees to stick to their own 'silo', is a company that will never have an effective cyber and information security system. Encourage employees to come forward with signs of breaches.

OUT-OF-DATE SOFTWARE

It's a huge security risk for your company, so be sure to keep software up-to-date.

Antivirus software is included for free with Windows and Apple computers, so enure this built-in antivirus is always switched on.

BE AWARE OF SOCIAL ENGINEERING

Employees are being targeted online on social media, social networking, and dating sites. This can lead to an individual's identity and credentials being stolen. It can even lead to theft, extortion, and blackmail targeted at your company. Be especially aware of people you have never met - this awareness is your single greatest protection. There are many other things you can do to protect yourself on social media.

Safety advice from Facebook, including info about online well-being and online consent is freely available from Facebook at: facebook.com/safety and from Be Safe Online at: gov.ie/en/campaigns/be-safe-online

Phishing

This is when you get an email that appears genuine with a file attached, or a link to click. This is the number one way for someone to get into an information network. Don't assume an email is really from the person it appears. It never hurts to make a call to check, especially if you're not expecting the email. And never click on a link in an email or a text that says 'your email has been compromised - click here to reset your password.' This is always a scam. If you think there's been a phishing email, investigate as soon as possible, don't leave it.

Tailgating

Tailgating is a physical form of social engineering. Many businesses are seen as 'soft targets' by those who want to cause harm online but also physically. Thankfully they are few in number but the threat of such people is real. An easy way for them to gain access is to follow close behind as someone holds the door open for them to a secure area. Anyone can buy a high viz or a clipboard to make it look like they belong in the building. So make it a standard procedure to always check the ID of anyone you hold a door open for, no matter how legitimate or official that person looks. And if you notice anyone who shouldn't be there or who's acting suspiciously, report it to security or the Gardaí but never place yourself in danger.

BE AWARE OF ONLINE AND TELEPHONE FRAUD

Invoice fraud

This costs companies, organisations, and individuals vast sums of money each year. Criminals find out about details of supplies, they fake an email with an invoice pretending to be from the supplier - or they fake an email appearing to be from a trusted colleague - and insert own fraudulent bank details. Watch for emails purporting to update banking details too. Always call the supplier, or the person who has asked for the payment, on a phone number you have on file (never the number in the email), and check if the details are legitimate.

Banking fraud

Your bank will never call, text or email asking for personal info, or asking you to move money. Ever. It doesn't matter how trustworthy the person sounds, it doesn't matter how much they know about you, what they say has occurred, or how they say it. They aim to instill worry, fear and a (false) sense of urgency. Put the phone down. Do not click a link or text message that they sent. Do not call them back from that phone if they invite you to because they will have compromised your phone. If you want to call the bank or the Gardaí use another phone and a legitimate contact number you already use or you find online - never a number you've been sent by email or text.

ONLINE VIDEO CONFERENCING

In an increasingly digital world, we are all online via video conferencing and this trend will continue for a long-time. So, to keep these meetings secure ensure you:

- Only include authorised individuals on the video call. Lock down the meetings to invited participants only. Question anyone who you may not know on the call, especially if their camera is switched off. Use waiting rooms for meetings.
- Generate unique meeting links and codes.
- Use only platforms with 'end-to-end encryption'.
- Never share links or codes on social media.

Digital Business Ireland

ONLINE RESOURCES

Ireland's National Cyber Security Centre has crucial advice on securely working from home

ncsc.gov.ie/pdfs/WFH-Advisory.pdf

A full range of online security information - on invoice fraud, CEO fraud, app security, banking security, online payments - and safe and secure online video conferencing - is available from the Garda Cyber Crime Bureau:

garda.ie/en/about-us/organised-serious-crime/garda-national-cyber-crime-bureau-gnccb-/

National Cyber Security Centre Ireland's effective and clear '12 Steps to Cyber Security' Guidance for Irish Business

ncsc.gov.ie/pdfs/Cybersecurity_12_steps.pdf

More information about the General Data Protection Regulation - which affects every single Irish business - is available from the Data Protection Commission

dataprotection.ie/en/organisations

With everyone working together we can create the safest possible online environment at home, and across Ireland, during the crisis and in the years that follow.

WHY SHOULD MY COMPANY CARE ABOUT CYBERSECURITY? - AN AUSTRALIAN LEGAL PERSPECTIVE FOR IRELAND:

The legal implications of cybersecurity for Irish companies and organisations are considerable, including:

- General Data Protection Regulation (GDPR) reporting applies to breaches
- Data Protection Acts
- Freedom of Information Act
- ePrivacy Regulations
- Companies Act
- Criminal Justice Act
- Criminal Justice (Money Laundering & Terrorist Financing) Act
- Criminal Justice (Terrorist Offences) Act 2005 (as of October 2020)
- Criminal Damage Act
- Criminal Justice (Theft and Fraud) Offences Act
- Criminal Justice (Offences Relating to Information Systems) Act
- Payment Services Directive
- Network Information Security (NIS) Directive.

Need to consider:

- How does this apply to me as a C-suite Board Director?
- What about Reputation / Insurance / Viability of operations?
- Consider Ransomware and Incident Response Plans and the effect on responsible governance.

Cybersecurity legal consequences for your business and organisation are huge. This is no longer a matter for the IT department; it is now a fundamental part of your legal and statutory obligations.

MESSAGE FROM STEPHEN RAE

Principal, Kobn European Leaders

Almost two years into the global Covid pandemic, Cybersecurity and Financial Crime are - like never before - now truly at the top of the agenda for every corporation and CEO. Organisations such as the World Economic Forum and the Financial Action Task Force (FATF) have pointed to the extraordinary increase in cyber attacks and money laundering – all under the cover of the pandemic.

Business is being adversely affected by the huge rise in fraud, online fraud and payments fraud. The Director of Public Prosecutions recently spoke to the IFPC2021 Cybersecurity & Fincrime conference about the "'industrialisation of fraud' which automation and the cyber sphere have facilitated."

If business and law enforcement are to be successful in tackling the fraudsters and cyber criminals it's now time to elevate cybersecurity and financial crime compliance as strategic business issues within organisations. But that is not enough; we also need to develop public private partnerships (PPPs) between industries, business leaders, regulators and policymakers.

Ireland has the opportunity to be a leader in Cybersecurity. Our geographical location between the EU and the US, our island status and the storage here of more than 30% of all of Europe's data provides a clear imperative to be fast adopters in this space.

Like Israel, for example, we have the potential to build campuses of excellence, say in Cork or Limerick/Shannon, where colleges, industry and even the Defence Forces can collaborate to build our Cyber Cities, akin to Be'er Sheva in the Negev Desert. With government support and policy changes our colleges can provide the skills that the private sector so badly needs.

The private sector will follow the skills and thereafter the colleges and tech companies can collaborate more deeply. With the involvement of state entities such as the Defence Forces, we will not only be strengthening our cyber defence capacity, but also building future entrepreneurs and latent generational knowledge.

We are however laggards on the international stage in terms of the importance that we place on Public Private Partnerships between law enforcement, government agencies and the private sector. That is certainly the case in fighting money laundering and economic crime. But PPPs also play a role in fighting bad actors in cyberspace. Only two years ago major cyber attacks were big news, rare events even. Today they are everyday occurrences and no longer attract big headlines – but the losses involved are staggering.

The far-reaching cybersecurity breaches of 2020, the widespread Solarwinds espionage event by a state actor on the United States, and the HSE ransomware breach of 2021 are a reminder to decision-makers around the world of the heightened importance of cybersecurity. Society has been conditioned to police actions being a deterrent to crime in the first instance; and where that does not succeed society expects police actions to detect those responsible. Astonishingly, in the cybercrime and FinCrime worlds this is no longer the case. Few cases are detected; the money lost is often lost forever; and the bad actors – State and criminal – face few sanctions.

Something has to change – and soon. Governments cannot afford for societies to lose faith in the authorities' ability to take action against organised crime and money launderers in cyberspace. But the efficient use of technology, Artificial Intelligence, risk based approaches, and improved policing methods can turn the tide.

Here's to Ireland grasping the opportunity to be leaders in fighting cyber crime and online fraud.

For Stephen's full analysis of today's fraud and cybercrime situation see: www.internationalfraudprevention.com

Digital Business Ireland

PROTECTING YOUR INFORMATION IN A DIGITAL ERA

A Cyber-Security Guide for SMES

www.digitalbusinessireland.ie