PLANNING IS KEY TO PREVENTING A CYBER BREACH

A cyber-breach is a major crisis situation for any business or organisation. While the threat cannot be eliminated it's important to put proper plans in place to respond to the breach, a panel of US cyber-security experts warned business leaders at a seminar in Dublin. Report by Grace Heneghan.

An insightful cyber-security discussion was recently organised by Arthur Cox in Dublin in association with the USA Embassy. Speakers included the Honourable John P Carlin, Assistant Attorney General for the National Security Division of the US Department of Justice, Sean M. Joyce, Principal Advisor to PwC, Virginia, and Jenny Durkan, Quinn Emanuel Cyber Law and Privacy Group, Washington State.

All three experts unanimously highlighted the need for a top-to-bottom review of all plans and protocols, which they said should be at the forefront of each and every company's strategy to prevent cyber breaches of confidential information and internal security systems.

As top national security attorney at the Department of Justice, John P. Carlin oversees nearly 400 employees responsible for protecting the US against international and domestic terrorism, espionage, cyber and other national security threats.

"People need to know and identify the cyber threats, and they also need to ensure that these threats are treated like a crime. If criminals steal information from private companies in order to compete against them then we treat it as theft," noted Carlin.

"A cyber breach is a major crisis moment for a company because your brand and reputation is on the line. If it's a national crisis, you need to know who to trust within your company and your government. Cyber criminals do not respect boundaries, so it can affect countless countries and regions."

Pictured during the 'Understanding Cyber-Risk' seminar (l-r): Jenny Durkan of Quinn Emanuel, Seattle, Washington; Sean M. Joyce; Principal Advisor to PwC, from McLean, Virginia, and John P. Carlin, Assistant Attorney General for the National Security Division of the US Department of Justice. (Pic: Jason Clarke Photography)

GROWING CYBER THREATS

Jenny Durkan is internationally recognised in the USA for her leadership in the areas of cyber crime, complex litigation, governmental policy and legislative strategy. She serves as Global Chair of the Quinn Emmanuel Cyber Law and Privacy Group.

"The security side of the technology has not kept up with the innovation of those who seek to do us harm. There's no greater threat to personal, business and national security than the cyber threat, and in the last three to six years this is happening more than we had envisaged. There's no business now in either the US or Ireland that is safe," she said.

"Ireland has made a name for itself in the technology sector where there's a greater accumulation of tech companies from all over the world, but mostly from the USA, who have this country its home for a variety of reasons.

"This not just for the tax benefits alone, but also because of the workforce here. If Ireland had a significant breach of one of its organisations this would have a tremendous reputational risk for the country as a whole and this would reverberate; it's a very competitive world and many countries would like to have that level of infrastructure and investment in their own jurisdictions," Durkan advised.

She recalled that upon initially starting at the US Attorney's Office she was given the "cyber hat" by the Attorney

General. "I started meeting the business executives of companies in Seattle because we have a lot of tech companies based there. During discussions with the IT departments, I found they would never tell me if they had a security breach, to save their reputation, and they didn't think they ever would need one, because they thought they were that good!"

NO COMPANY IS SAFE

But Durkan also warned that regardless of region or country, no company is safe from threat. "Sharing information is critical in order to protect your business and your employees. Otherwise, you are giving advantage to the people who are trying to do you harm.

"As the fifth of eight kids in my family the best thing is you learn from the mistakes of your siblings. So, we now know the current playbook for some of the biggest breaches of security, and know which ones have been successful and the ones that didn't work."

Every business that does not take the steps to prevent those known damages will find itself in bad shape, she warned. "There are things to be done from both an operational and management standpoint to be in the best position possible, and if there is a breach, be ready so less damage is done to your company. When you're in the middle of the storm it's not the time to ask where the shelter is, because that should have been planned out in advance."

AN ENTERPRISE RISK

The cyber threat is an enterprise risk – it's not an IT risk – and is something that chief executives and chief operating officers in every company should be very concerned about, warned Sean M. Joyce.

Prior to PricewaterhouseCoopers, where he is Principal since December 2013, Joyce served as Deputy Director of the Federal Bureau of Investigation since September 2011, with oversight of the FBI's 36,000 employees and an $8bn budget.

"During his visit to Ireland, Sean Joyce said he visited with several companies, and was very interested to hear their understanding of the current

TOP TEN EXPERT TIPS ON MANAGING CYBER RISK

1. **Do Not Delay:** There is no greater threat to business than cyber-threat. Doing nothing is not an option. Deal with it. Do not put this to the bottom of your 'To Do' list. Cyber-threat is not an IT problem: it is an enterprise risk. The operating assumption should be that no business/organisation is immune from attack.
2. **Planning Is Key:** A cyber-breach is not just 'a breach': it is a crisis. It can mean life or death for a business/organisation. While you cannot eliminate the threat you can plan how to respond to a breach. In the middle of a storm is not the time to ask where the shelter is!
3. **Road-Test The Plan:** How will it work in practice? Think through all the various contingencies? How will a breach affect the business/organisation? Can you shut down your information and communication systems safely? How will you deal with regulators? Who will be your spokesperson? What will you do to minimise litigation risk?
4. **Get Everyone Around The Table:** Everyone who will be involved in responding to an attack should be involved in planning for an attack. Get the right people around the table. The day of the crisis is not the day you should be meeting your advisors for the first time.
5. **Government and Garda Contacts:** In the event of an attack, you may need to liaise with the Government and An Garda Síochána. Ensure you have the correct contacts, otherwise you will not have an effective plan.
6. **What Needs To Be Protected:** What is of most value to the business/organisation? Is it intellectual property? Is it confidential business information? What are you doing to protect this information? Consider putting in place a naming convention only understood by limited internal personnel.
7. **Review All Third Party Suppliers/Service Providers:** Carry out a comprehensive due diligence exercise. Review all contracts: Are your suppliers/service providers required to follow a cyber-security framework? What are they required to do to protect your information? Are they required to inform you if their systems have been breached?
8. **Raise Awareness Of The Threat:** Ensure that all personnel understand the scale of the threat and are alive to the most common forms of attack. Do they know what 'spear-phishing' is? Do they know who to contact if they receive a suspicious email? Roll-out training across all sectors of the business/organisation.
9. **Print Out The Plan And List Of Key Contacts:** All key personnel should have a hard copy of the plan and a laminated card of key contacts and their contact details. Remember, when you are in crisis mode, you may not be able to use your information and communications systems. Make sure this plan and your key contacts are reviewed and updated regularly. An out of date plan in a crisis will hamper your rescue.
10. **Be Open About The Breach And Learn From It:** Talk to Government and Garda contacts immediately. Information sharing is critical to protecting not just your business, but the economy in general and Ireland's reputation abroad as a great place to do business. If you do not learn lessons from a breach, you are opening the business/organisation up to potential liability in the event of a further attack.

risks out there. Risk is about impact and probability, how many of them understood that as nation states, terrorists, organised crime and criminals, activists and insiders, and to identify the risks to their specific companies. What valuable assets are important to the company that could risk and affect the reputation and brand of the company? I was greatly surprised that these companies were asking me if they were at risk because they're based in such a small country as Ireland!

"It's disappointing to me that you are not able to see, much like US citizens, the threat intelligence that we receive every day of what nation states are doing to our economy and your economy; they are basically taking our competitiveness and some of our economic gains, and replacing it by putting theirs in the forefront. This threat is very real and all companies need to address it from the top down," noted Joyce.

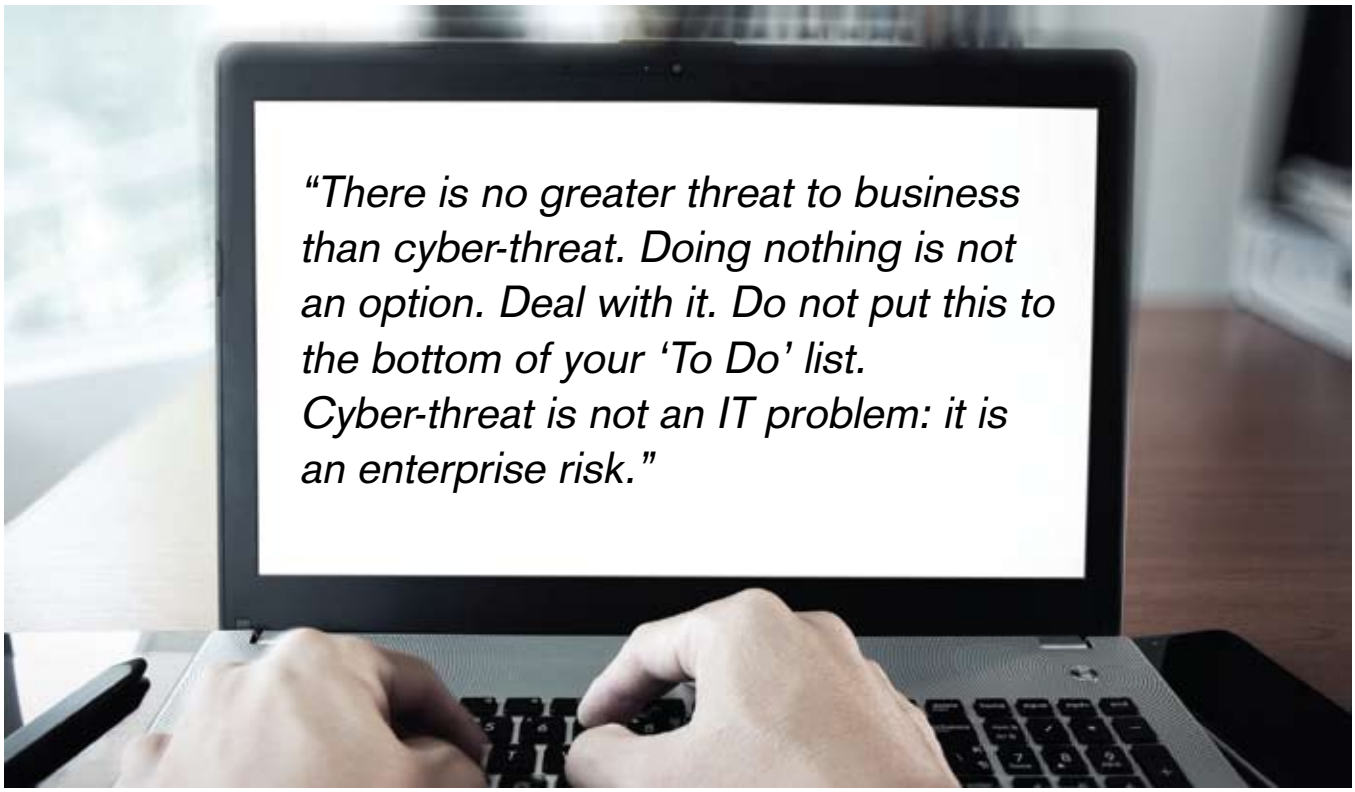
Spear phishing is an email that appears to be sent from an individual or business that you know. But it's actually from the criminal hackers.

CYBER-DASHBOARD

Regular updates, he said, were needed but if there appears to be a communications issue and a lack of understanding in the boardroom; from an enterprise risk perspective, the board then needs to have the company's framework perspective and the roadmap in going forward.

"I recommend a cyber-dashboard to identify any significant breaches that warrant the attention of the high level members of the company, and then look at the financial plans and training. But there is a definite lack of understanding. How many people know what spear phishing is? You need to do the basics – check if your network is segmented, and if you are receiving threat intelligence. The board's role is in an oversight capacity to ensure the house is safe, so that the alarms are working, have been tested and are working properly.

"This cannot be done in isolation and takes a partnership between the public and private sectors. The USA has done



a good job and there are now many bi-sectoral information-sharing analysis centres, such as the National Cyber Forensic Training Alliance, National Cyber Investigative Taskforce and the local FBI and secret service offices.

"So, one of the mechanisms Ireland needs to take on board is a dual partnership – companies here can be successful and be in a 'protect-prevent' mode rather than a 'react' mode."

SPEAR PHISHING

Operational reviews will keep track of invaluable information, so companies must do a 'top-to-bottom' review and do penetrating testing of the system, Durkan claimed. Pointing to the new threat of 'spear phishing', she said this has led to some of the significant breaches to date.

Spear phishing is an email that appears to be sent from an individual or business that you know. But it's actually from the criminal hackers who want credit card and bank account numbers, passwords, and the financial information on your system. "Once you click on the information link in the email this will download a malware, and the virus accordingly copies the financial data and confidential company information," she pointed out.

In their concluding remarks, all three speakers agreed of the vital importance to put an effective plan together in going forward. They pointed to the need for all parties, internal and external, to attend all table-top exercises.

It was incumbent, they maintained, upon CEOs and the board of management in each company to be ready for any threat and take those basic steps to best protect the company, so they are prepared in the event if something does happen.

The take-home message for all companies was that whilst they cannot stop all of the threats, they can stop many of them. Forward planning is critical to any company's survival.