KEEPING SUPER SAFE

GNGB recently held a roundtable for our Security Committee members with cybersecurity specialists from Deloitte Cyber. The discussion looked at why cyber threats have vastly increased during the coronavirus crisis; what types of activities are most common; and how companies can keep their systems and information secure while most of their employees are working from home.

Special guests:

Tommy Viljoen, Partner

Tommy has more than 25 years' experience in leading and developing cyber security, privacy and risk consulting services to a distinguished financial services client base. His focus in Australia over the course of the last ten years includes working with some of the largest insurance, banking and wealth management firms and developing strategies and implementing cyber solutions.

Vijay Pasupathinathan, Director

Vijay is a cyber security advisor helping organisation improve their cyber security and risk practises. Vijay has over 16 years' experience in leading and delivering cyber security programs and transformations, establishing cyber risk management practices, leading managed service operations and serving as a trusted adviser to business and technical stakeholders.

THE DEVILS WE KNOW

Through their global network of cyber intelligence centres, Deloitte has seen a surge in cyber-criminal activity since the onset of the COVID-19 pandemic. Interestingly, the malicious actors are not new to cyber specialists – the same groups they've been familiar with over the years are just much more active as they find, and exploit loopholes created by the pandemic.

LOOPHOLES LARGE AND SMALL

The industrial world has never seen such a monumental rush for the exits as we have this year. One Big Four bank alone sent 20,000 people to work from home over the course of just two weeks. Programs of work that previously would have taken a year or more with planning, gradual roll-out, testing and recalibrating, have been executed in a fortnight or less. And as we have moved our lives online, the bad guys, who were already in residence, have had a field day.

These criminal actors are from all around the world and using 'commodity' malware that has been around for years are targeting the large remote workforce. Far from being sophisticated attacks, hackers are using old tricks to exploit the new vulnerabilities.

OLD DOGS WITH OLD TRICKS

Our thirst for information about the pandemic has allowed attackers to lure us into traps much more easily. Our inboxes and browsers are full of information from sources we haven't previously engaged with. And that's a breeding ground for cyber-attacks.

- **Social engineering and spoof domains**. Digital communications have increased exponentially. We are all clicking on websites we haven't been to before, and often connecting and talking to people we haven't spoken to before. Just one example is – there were 4,000+ attempts to set up websites that have some sort of affiliation to WHO and divert information through to those websites to phishers. Once a user clicks, their computer can be remotely taken over or their information stolen. Zoom has been the target of numerous cyber-attacks, with fake Zoom links leading unsuspecting users to take malware onboard. Office365 has also been targeted, with fake security pages allowing hackers to take control of users' computers.
- **Cloud-based attacks**. As we move to the cloud, so do the hackers. While cloud storage is typically very secure, the entry points - how organisations are connecting to, setting up and using cloud via APIs and other mechanisms – are leaving lots of vulnerabilities for attackers to target.
- **Network attacks**. As companies introduce new VPNs and make big, fast changes to routers and networks, portals have accidentally been left open and organisations have been attacked.
- **Patch failures**. In the rush to organise work-from-home, organisations have not been patching their software adequately, leaving the door open for criminals.
- **Home router hijacks**. Attackers are targeting our home DNSs and targeting all traffic. These attacks are typically 'symptomless' so unless you know what you're looking for, you can be working away at home completely unaware that all your data is being observed in the background.

GETTING REAL

Deloitte's cyber centres see real world attacks every day. Three recent case studies from COVID-19 times have been:

Pirate Panda: a COVID-19 themed attachment to drop a six year old malware application called Poison Ivy Remote Access Tool – ancient in internet years – into any computer via email. The file is a WLL file, a Microsoft add-on, which executes every time MS Word is opened. This allows hackers to perform screen capture, password theft, file transfer, system administration, and traffic relaying. Hackers cast a wide net, capturing anyone they can, both home and business users.

APT36: A malicious Excel file with malicious macros introduces Crimson Remote Access Tool allowing information stealing, data extraction, file retrieval and more in a 'spear phishing' attack.

Office365: An executive within an organisation that had moved very quickly to Office365 received an email asking them to input their credentials to access urgent documents awaiting review. The web page looked exactly like the typical Office365 credential set, but the malicious software redirected the executive's email outside the organisation and allowed the malicious actor to access all of their drives.

THE BEST PROTECTION

So how can we protect our own organisations? The steps aren't complicated, but they do take work. The top three are:

1. **Educate educate educate**. The information you provide to users on what to be careful of, what to do, and what not to do, the better off your firm will be. Education is the cheapest risk management tool by far, so do whatever you can to warn your users, and provide guidance on what they need to watch out for, and what they need to do if they see something untoward.
2. **Patch and harden your infrastructure**. In these times it's difficult to keep up with the pace of change, but it's important to make sure anything your organisation introduces is securely configured and patched. Go overboard rather than risk leaving gaps.
3. **Detect.** A lot of organisations have spent a lot of money on securing their environments, but then don't have the firepower to know when something is going wrong. Having the ability to detect when things are not on track is really important at this time.

SO NOW WHAT?

How organisations respond once threats are detected is the key to the city in terms of avoiding lasting damage. Deloitte identified nine steps to respond, react and recover from a cyber-attack.

1. **Prioritise**. If you're having to open up your networks, make sure your priorities are around what controls you're going to provide, and what education you're going to give your users.
2. **Share threat intelligence with other organisations**. We've seen great communities coming together to share information, notably among the banks, and among the property companies. We all compete against each other but when it comes to cyber, it's not a strategic advantage. So the more you communicate and share information, the better off everyone will be. Joining the GNGB security committee is a great place to start!
3. **Use intelligence to move at speed**. If you hear about a threat via Office365, go and check what your configuration is, what APIs are next to your system. Look at where emails are being taken out of the organisation, and if you've got emails being sent to the same address in large volumes, check whether that's appropriate or not.
4. **Focus on known tactics**. For example, we know that any site that has WHO on it and is asking you to click, is likely to be a scam. Knowing where the targets are, being aware, and informing people about what's happening makes your organisation more robust.
5. **Optimise detection**. On average, it takes over 200 days between malware landing on your system and you detecting what's going on. If you don't have the right mechanisms in place it could be there for a year or two and you won't even know you're being observed. Improve and increase your monitoring and mechanisms to detect what's happening. That includes your cloud environments. There's a misperception that once things are put into AWS or Google Cloud they're safe, but it's in the connections to the cloud we are seeing issues. The ways organisations are connecting to, setting up and using cloud are leaving lots of vulnerabilities and holes.
6. **Check your email.** Email technologies are vulnerable as gateways to organisations and executives so it's really important to monitor them closely.
7. **Update the playbook**. Our playbooks are not fit for purpose for today's environment. You need to decide what you need to do to respond to the conditions we are under today.
8. **Have a recovery plan.** Toll showed us how a serious attack can take down a business completely. Have a plan, not just for one or two systems, but for rebuilding the whole system if you need to.

Working from home SECURELY

Remaining vigilant for cyber threats while working from home keeps company and customer data secure

Devices | Network | Scams | Data | Incidents

Protect devices & Network

- Reset the default password for your router and limit use of your network to your household
- Keep your credentials private and secure
- When appropriate, connect to the VPN to prevent outsiders from intercepting your online activity
- Remember to lock your device when you step away from your work area
- Use surge protectors when charging your devices
- Keep devices out of reach of younger family members and pets

Protect from scams

Recognize official messages, look for proper domain names and consistent grammar and formatting

Spot phishing emails by looking for the following:

Unexpected urgency

Unusual senders

Request for sensitive data

Protect data

Only use approved communication channels and tools to share company and client information

Double check recipients before sending an email

Report incidents or concerns

"Programs in my company-provided device are opening and closing without my input"

"I inadvertently sent an email with confidential information to the wrong recipient"

"I received a suspicious email from an unknown sender and clicked on a link"

"My company-provided device was stolen and I can't locate it"

Source: Deloitte Cyber 2020