Over the last decade or so, we've always found the first quarter of the year to be a quiet one. However, change is the only constant, and this year began with a bang. There's lots of activity across the industry and it's enlightening to see a marked increase in the level of executive awareness of the need to secure sensitive information and critical systems. Thanks for taking the time to catch up with us – some key highlights in the industry for this quarter are below.

The health sector – time to get our act together

The banking industry has been waging a war against cybercrime for decades (with the big 4 banks typically employing 200+ focused in security alone), and 2014 was noted as "the year of retailers getting hacked over and over again". We unfortunately think the healthcare industry is the next cab off of the rank.

This quarter, an excellent study was released in February titled "Securing Hospitals". Although its title seems limiting (and US centric), it nonetheless does an exceptional job highlighting the diverse risks our health sector faces in today's digital world. It illustrates that not only "patient records" are at risk, but "patient health" itself. What makes the industry unique is that it not only faces the 'traditional' information security risks of Confidentiality, Integrity, and Availability, but also has to deal with the exponential growth of internet-connected health devices and industrial control systems (see connected medical devices, apps: are they leading the iot revolution – or vice versa).

As a Non-Executive Director of a listed health-based organisation said "if a bank loses my money, they can give it back to me... but if we lose someone's private health information, we can't just give it back - it's gone for ever". The implication was that the organisation should therefore be 'above bank-level' security. Yet achieving that level has its challenges. The Securing Hospitals study also highlighted the 'common design issues' that fail many organisations. Locally, the recent virus attack that "crippled Royal Melbourne Hospital Pathology" due to using an obsolete (Windows XP) operating system, highlighted the practicality of those design issues.

As a segue to the next item, one senior IT pro from the health sector pointed out to us recently that a large number of their hospital-based, vendor-provided access systems (aka Industrial Control Systems) had similar, obsolete operating systems embedded into the overall systems they were installing...

Hacking the Ukraine's Power Grid

In January, a group of 'white hat' Russian security researchers published their "shame list of industrial control equipment" (used in the healthcare sector, amongst many others). This is a list of "*...equipment, used in various industry fields, which comes with simplistic default administration credentials. These admin logins are shipped with every product, and they are detailed in each product's manual."*

While we're on the topic of Russia and control systems, this quarter also saw one of the first significant attacks on a country's critical infrastructure (Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid). It's a gripping tale:

"The [company's] operator grabbed his mouse and tried desperately to seize control of the cursor, but it was unresponsive... the machine suddenly logged him out of the control panel. Although he tried frantically to log back in, the attackers had changed his password preventing him from gaining re-entry. All he could do was stare helplessly at his screen ... eventually taking about 30 substations offline. The attackers didn't stop there, however. They also struck two other power distribution centers... nearly doubling the number of substations taken offline and leaving more than 230,000 residents in the dark."

We have the practical, project-based experience to say that these issues are both real and probable. However, to be fair, we thought you might also enjoy the contrarian's view point that was published this quarter on how "Squirrels are a bigger threat than hackers to US power grid"

Will ‘personal comfort’ bring down a presidential candidate?

Unfortunately it’s not Donald Trump, but Hillary Clinton and her email scandal which is getting considerably hotter as the US presidential election gets closer. A recent article in the Washington Post is a very good read (here). To reinforce the political reality of the issue, a former white-house cyber security advisor, told us on a recent visit to Australia that “indictments are inevitable”. It seems there may be good reasons why there are “dozens of FBI personnel deployed to run down leads” as the article states.

However, on a more practical, day-to-day level we think this article highlights one of the most fundamental issues and challenges facing organisations today. On one hand, the article notes “the issue here is one of personal comfort” (for a reason why she bypassed traditional approaches). While on the other hand, it highlights that her role as Secretary of State and the content of those emails were highly confidential, and that she went out of her way to avoid the constraints that she apparently thought were unnecessary. The ‘old school’ security team simply says NO (as implied what also happened in the article), so as we all know, senior and/or creative staff figure out how to do their job irrespective. The “new school” security team has to work harder to find ways to help the business grow and be innovative, yet do so securely. It’s often easier to say NO, than to understand HOW... drop us a note if you’d like help with that very challenging problem.

$5.3 million – a big phish that got away...

In March we learned that a phishing attack nearly cost a US regional bank $5.3 million! In the past few months, thousands of organisations have fallen victim to the recent wave of ‘ransomware’ such as the Hollywood Hospital that was held for ransom for $3.4 million. It’s frequently noted that an organisation’s ‘weakest security link’ are the well-intentioned employees who fall prey to cleaver email attacks.

For that reason, we developed a simple, well-designed approach to conducting a safe, but effective phishing attack to provide senior management with factual insight. We often know it’s a risk, but infrequently quantify it. For example, one recent project found almost 40% of staff clicked on an insecure link. Even worse, 37% actually provided us with their username and password. This information becomes an invaluable baseline to evaluate the effectiveness of a tailored employee awareness program and overall risk profile. Drop us a note here if you’d like to learn more about our unique “Analytical Cyber Health Statistics for fact-based Decision Making”.

Salient Statistics...

Each quarter we trip across a wealth of statistics published from diverse sources. When used sparingly and in the right context, statistics can often improve a discussion with senior executives or those less exposed to the industry.

- 75% of corporate boards are not actively involved in cybersecurity oversight (includes 5 good questions every CEO should ask about cybersecurity)
- President Obama’s proposed US$26.9 billion infosec budget, would make it the 10th largest Australian company by market capitalisation (ASX market cap at the end of Mar 2016).

Thanks for investing the time to read this quarter’s newsletter. Please feel free to pass this along to anyone who might find it of interest (or they can subscribe here).

TrustedImpact
PROTECTING DIGITAL

we’re **independent** consultants – it’s about **your** business and **your** success
with a **singular focus** – information security is all we think about
leveraging **experienced** professionals – credentials, not checklists