
It's the season to reflect upon things that are important, and you're one of those things. We appreciate you taking the time to read our newsletter and we thank you for being a friend, colleague, or valued client (or all the above!). We hope your holiday season is safe and filled with family, friends and fun!

## Lifting our game in 2018, so that clients can lift theirs!

In 2018, Trusted**Impact** is formally launching Security**Thinking**, a suite of human-focused services including security awareness programs, phishing detection exercises, crisis response, positive security influence and executive-focused knowledge.

Why? A multitude of studies highlight "Insider threats as the main security threat in 2017". We find staff susceptibility is a real issue from client projects that we perform. For example, a database of results for client "phishing exercises" found that **84**% of employees who read our phishing emails not only click on a nefarious link, but also provided us with their username and password. Furthermore, a majority of our "red team / capture the flag" exercises are successful by employing social engineering techniques against unaware staff in order to obtain their credentials.

Thus, we're delighted to announce our formal partnership with a global leader for Information Security Education – Canadian-based, **Terranova Corporation**. Terranova provides simple, engaging and effective security capability programs for organisations of all sizes. It's not just about providing engaging education programs, but combining those programs with powerful ways to effectively distribute targeted awareness programs to staff, and measure progress as part of a more strategic cultural change effort.

A quick overview is here, and if you'd like to discuss how to more effectively improve your Security**Thinking** capability, just drop us a note here.

## Reflections of 2017

It was a big year in our industry. Since it's that time of the year, we thought it might be worthwhile reflecting on the major headlines in 2017 as a potential sign of things to come. Two key themes involved:

1. **Exponential Cybercrime.** Last year, we thought the $3 Billion in losses to the "Business E-mail Compromise" scams and ransomware was large... that was until we learned that this years' estimates are $5 Billion, or 15 times larger from 2015. When organisations are forced to pay ransomware amounts of $1 Million (the largest known payment for ransomware), it's not hard to imagine why the total cost of cybercrime is now expected to hit US$6 TRILLION by 2021.

   It was well put by CSO Online when they noted "This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined.

   ***The message:*** *If Confidentiality, Integrity, or Availability of your organisation's data or systems is a defined risk on your company's risk register, consider adding it in greater detail and increasing the "Likelihood" rating of an event. Your Board is kidding itself if they think it's a question of "if" an event will happen, and not "when" it will happen.*

   *Furthermore, the executive group should be conducting "cyber crisis exercises" to identify how to improve your ability to respond and recover. We've got lots of experience helping organisations conduct coordinated, cross-functional cyber crisis exercises. Drop us a note here if you want to find out more.*

2. **The C-Suite ramifications of an incident.** Australia's mandatory data breach notification scheme quietly received royal assent approval in February of this year. The new law takes effect in February 2018, and a good resource for your reference and obligations is here.

Globally, the C-Suite saw considerable pressure with last quarter's Equifax data breach. A good article here, highlights how the Equifax breach is different than most, and which provides 5 key lessons. Indeed, the scrutiny continued this quarter when the company's former CEO (note: he became 'former' because of the breach), was publicly berated by lawmakers who stated "I don't think we can pass a law that fixes stupid". That said, it didn't stop lawmakers from introducing a bill in the US that seeks jail time of up to 5 years for executives who hide data breaches. We suspect the executives at Uber, who apparently paid hackers $100,000, would be slightly concerned if that bill makes it into law.

***The message:*** *Not only should you consider increasing the "Likelihood" of a cybersecurity event, consider also increasing the "Impact" to a level commensurate with your (changing) legal obligations and level of executive exposure (not just an IT problem, but a business problem).*

These trends were further corroborated locally when the Australian Cyber Security Centre released their "ACSC Threat Report 2017" in October. They highlighted that two of the significant ways that the environment has changed were the "frequency, scale, sophistication and severity of cyber incidents" and "more diverse and innovative attempts to compromise government and private sector networks". Risks are increasing – don't be complacent.

## Focus on the basics in 2018

A good sports team becomes great because it executes "the fundamentals" extremely well. The same is true for your organisation. For example, the Australian Signals Directorate's "Essential Eight" reinforces the basics and good cyber hygiene.

Yet we often find there's still plenty to do, as highlighted this quarter by a UK survey that found 1 in 4 company system accounts were inactive. Unfortunately we found it was even worse this year when we conducted a number of 'health checks' that analysed user accounts to help our clients improve their cyber maturity. With approximately 113,000 system accounts analysed in total, 2 out of 5 regular accounts (40%) had not been accessed for a year or longer. Even worse, when we analysed the "privileged" accounts, we found more than 1 in 3 were inactive and nearly 60% were 'adjusted' to remove password expiration.

Don't accept the typical response "our policy doesn't allow that to happen" – factual insights often prove contrary. Do you know your numbers? Drop us a note if you want help gathering them.

## Significant Salient Statistics...

This quarter's statistics come from PwC's 2018 Global State of Information Security Survey. It also reinforces the need to focus on the 'basics'... its survey of 9,500 exec's from 122 countries found there's still lots to do:

- 44% said they do not have an overall information security strategy,
- 48% do not have an employee security awareness training program, and
- 54% said they do not have an incident response process.

---

We're privileged to have worked with some great clients this year and help them resolve some difficult cyber issues. We look forward to reconnecting with you in 2018, and appreciate you being part of our community. Please feel free to pass this along to someone who might find it useful (or they can subscribe directly here).

Kind regards,

TrustedImpact
PROTECTING DIGITAL