Fourth quarter update
December 2014

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 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 fellowship!

Just when you think it won't get any stranger…

Was it North Korea? Was it staged by Sony? Was it "Lena" the insider? Everyone seems to have a view (including the humorous tweet from Kim himself). Instead of wading into the mess, we thought we'd simply reflect on 3 key lessons learned from the Sony Pictures hack that may be relevant to you or your organisation.

The first is gaining an appreciation for the threats your organisation may face. We recently advised a Board of Directors that their security posture should reflect 'who in the world, wants your data, and why'? The 'threat' aspect of a risk assessment is often overlooked and motivations can change dramatically between companies and industries. It can also change over time and your risk thinking should reflect major events. While this was the release of a movie, more mainstream examples include acquisitions, going public, or making a major market announcement.

The second lesson is the age old "ticking time bomb" called the company 'share drive'. You know, those massive corporate cesspools of data that many organisations maintain. Access to this type of data was evident when we learned about the 2005 era spreadsheet providing Deloitte salaries, and the gigabytes of Sony data that were exposed. One of our savvy clients ruthlessly removed a number of old files from their share drive, and are still waiting to hear anyone complain. They're also trying to break the 'one massive' share drive into smaller, more manageable drives. As a parting question on this lesson, would you be alerted if gigabytes of data were exfiltrated from your network? We've helped define a number of 'monitoring' strategies, if that would be of interest?

Finally, the third lesson is the importance of incident ~~planning~~ 'training'. As one of our favourite infographics show (see information is beautiful), there isn't a lot of commonality behind who, why or how a data breach occurs. However what DOES separate those organisations is the dramatic difference between those who react versus those who respond. For example, one of our monikers has been 'these days, getting hacked or having a data breach is inevitable… becoming a headline doesn't have to be'. It's not simply about getting all parties into the same room to do a 'what if' scenario (although that's a good start). Consider multiple scenario's, leverage experts and think through things like how quickly to respond and with what level of detail. Most important is the subtle, but significant difference between planning and 'training'. Incident planning shouldn't be a once off event – practice, or 'training' can pay off in the event of an incident. Drop us a note if you'd like a 'personal trainer' or would like to explore how it might work in your organisation.

Just the numbers…

Every 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. Therefore, we thought it might be of value to you to simply compile a few interesting statistics that we see each quarter. This quarter we found these found these interesting:

- This quarter, the world counted over 3 BILLION internet users. That's one large group standing on your digital doorstep.
- 42.8 million Security incidents were detected in 2014, or 117,339 per day – a compounded annual growth rate of 66% since 2009.
- 45% of holiday shoppers will avoid stores that got hacked
- 48% of eCommerce sites lose financial data to cyber criminals and only 53% 'make every effort to keep anti-fraud measures up to date'.

- More than 26 percent of [file share] applications are being used by various business functions without the IT department's approval or knowledge.
- Home Depot spent $43 million on its data breach in one quarter alone… it's facing 44 legal actions filed in courts across the US and Canada
- 78% of global dealmakers report that cybersecurity isn't a part of the due diligence process before mergers and acquisitions

The (digital) company you keep?

This quarter we noticed a Distributed Denial of Service attack 'stopped Sweden working'! Purportedly it was part of an attack on a different part of Sony, for which details are still emerging. But it seems that Sweden's largest ISP, Telia was collateral damage. "*Telia were not the prime target. It was an internet gaming company that was attacked and they sent us massive traffic which our DNS servers could not handle*."

Granted, Telia only have 1.2 million residential subscribers. Nonetheless, this story highlights a practical issue we often see and that will become even more prevalent as cloud adoption grows. For example, we conduct a large number of website 'penetration tests'. Often we find medium sized or smaller organisations sharing their web infrastructure with hundreds of other sites. Shared infrastructure and many aspects of the cloud offer considerable value, but the possibility of becoming collateral damage because of your 'other digital tenants' is worth considering when weighing the advantages and risks. We've got a wealth of cloud-specific risk credentials if you'd like to explore practical cloud risks further.

Setting and managing practical expectations

Late last year saw an example where a range of security issues (amongst others) lead to the resignation of the Obamacare CIO. It seems that this year someone was trying to keep track, and recently highlighted that here were eight breaches of 2014 that costed a job. A disconcerting outcome in an industry where the risks are varied and dynamic. It highlights the importance of setting and managing expectations across a diverse range of stakeholders. We think we're fortunate to have a unique breadth of information security exposure across thousands of projects and hundreds of clients. Just drop us a note you'd like help communicating the practical 'state of global / local security' to your executive team.

The year ahead?

It's that time of the year when predictions are pervasive. One technology-oriented list of 'Top 10 Tech Industry Megatrends of 2015' caught our eye, not because of its outlandish insights, but simply that six of the ten had direct or significant security implications!

Thanks for being with us in 2014 and investing the time to read this quarter's newsletter. We wish you a happy new year and prosperous 2015. Please feel free to pass this along to anyone who might find this of interest (or subscribe them here).

Kind Regards,

TrustedImpact
PROTECTING DIGITAL