VIRTUAL GOLD AND CYBER OUTLAWS IN THE NEW DIGITAL FRONTIER

TrustedImpact - Head Office: Level 9, 22 Albert Road, South Melbourne VIC 3205
secure@trustedimpact.com (03) 9023-9710

New thinking for the New Digital Frontier

We're nearly there! Last decades' promise of the information superhighway is now a practical reality. Internet speeds are growing exponentially; small, affordable and mobile devices fit neatly in our pockets with more computing power than Apollo 13; and the 'cloud' gives us data and information anywhere, anytime. We call this the 'New Digital Frontier' because it's the recent confluence of these trends that's fuelling the explosion of connectivity and opportunity.

Virtually every organisation - either large or small, commercial business or government department - is racing to become more and more "connected" in this New Digital Frontier – and it's providing unimaginable opportunity for those organisations that can get there fast. It's also providing unimaginable opportunity in other 'new' areas that also didn't exist a decade ago – in particular, cybercrime.

In today's highly connected information economy, data is the new 'gold' and the ability to turn it (data) into hard cold cash has also become easy. Massive concentrations of data are being captured and stored online by many organisations: forming powerful targets for online criminals.

Cybercrime's now bigger than the global black market for marijuana, cocaine and heroin. In March 2012, the Director of the United States FBI formally announced that "the cyberthreat" would soon overtake terrorism as the number one threat, and he believes "there are only two types of companies: those that have been hacked and those that will be." Simply put: Cybercrime's real, it's big and it's growing very fast.

Directors and CEO's leading the charge into the 'New Digital Frontier' must make sure their organisations think and act differently to minimise these new and evolving risk of cybercrime. As discussed further, traditional 'bricks and mortar' thinking simply doesn't apply in the New Digital Frontier. Organisations racing to the New Digital Frontier must think differently and heed Darwin's challenge to "adapt or die".

The New Digital Frontier

The Internet represents an exciting 'New Digital Frontier' for almost every organisation. Businesses, government departments and organisations of all types are taking advantage of the New Digital Frontier to connect with customers, constituents and the public at large.

It's rapidly expanding and self-propelling a mass of tightly connected web sites, smart phones, tablets, and offers a new world for connecting, sharing and transacting.

Something that started as an interesting way to share university research material is now pervasive throughout almost every aspect of people's lives all around the world.

Why are so many organisations venturing into the New Digital Frontier? The answer is simple: Unprecedented Opportunity! This opportunity comes in many forms to suit almost every type of organisation.

For example, much faster Internet speeds mean you can now provide your customers with a responsive, feature rich experience. It wasn't too long ago that simple pictures painted slowly down one's computer screen, but now video can stream to computers as fast as it does to TVs. In fact, between 1990 and 2010 Internet speeds have increased by a factor of 10,000 [1]. This now means this channel is both rich in content and low cost for many organisations.

In addition, increased mobility via smart phones and tablets now puts the traditional 'customer service rep' or front line employee into the hands of your customer every minute, of every hour, of

[1] *http://www.techknowtimes.com/web/download-speeds-through-the-years-an-infographic/*

every day. Innovative organisations are engaging in meaningful connections with their customers on a 24x7x365, global scale.

Rewards for organisations able to innovate online are major. It provides: strategic advantage over competitors, global reach beyond traditional geographic boundaries, increased market share and share of wallet, and the potential for a lower cost delivery channel.

"Let's face it, every business today is an internet business. Try doing business today without a web site and you're toast…

If you're in retail but not selling online, you're in for a world of pain as Harvey Norman and David Jones are discovering as young upstart internet retailers… eat their lunch"

(Matt Barrie – BRW 08 Feb 2012, www.brw.com.au/p/sections/fyi/matt_barrie_start_up_success_A7ILMgWkKQ6YA3xbbWwlFP)

Why new thinking is needed

Just like venturing into any new frontier, there are new conventions, different behaviours and emerging threats.

Operating in the New Digital Frontier is very different to the 'bricks and mortar' world. For example; establishing customer relationships remotely, delivering 'straight through processing' and services automatically, providing product downloads instantaneously, and protecting digital assets are just some of the important differences. Recognising and adapting to this new environment is crucial for survival.

Consider the story of the explorers, Burke and Wills. In 1860, they led an expedition to travel more than 3,000 kilometres across Australia. They had considerable support and resources to back them up. Leaving from Melbourne, they took a large team of experienced men, horses, wagons and camels plus a large supply of food. The last section of the crossing, however, involved Burke, Wills and one other (King) travelling separately. In the severe conditions of the desert, Burke's and Will's traditional thinking, approach and preparations fell apart. Burke and Wills were unable to adapt and they perished. King, however, got help from the local Aboriginals who knew how to survive in this 'new frontier' and survived.

The inability adapt to the different threats they faced was the difference between life and death for these, and many other explorers of new frontiers. Similar could be said of organisations venturing into the New Digital Frontier: methods and thinking used in the traditional "bricks and mortar" world will not succeed on the Internet. Failure to challenge assumptions, rethink methods, and adapt to the different conditions and threats will be damaging to an organisation's reputation, brand and bottom line.

A New Breed of Cyber Outlaw

Whenever new frontiers have opened throughout human history, criminals and outlaws have flourished, and the New Digital Frontier is no exception. But instead of riding on horseback and holding up stage coaches, 'cyber outlaws' are harnessing the power of the Internet itself to build sophisticated and profitable online crime businesses.

Consider this. Anyone who is somewhat enterprising, IT-savvy and looking to make a quick buck can now earn a reasonable living targeting organisations anywhere in the world - without even leaving their home.

With many organisations storing large volumes of valuable data (customer details, financial data, credit cards etc.) online, they just need to work out how to get it. And that has been made easier with readily downloadable 'DIY hacking kits' that take the 'geek' factor and hard work out of becoming an online criminal. Faster broadband speeds also make it so much easier to launch large-scale attacks and then to get away with the proceeds by instantly shifting large data volumes across the globe. In fact, through automated hacking techniques (such as creating 'web bots') they can virtually 'hack while they sleep'.

To make matters more difficult, it's very difficult to coordinate across countries and geographies with diverse laws, legal frameworks and policing bodies. If an online criminal operates from offshore, the chances of being caught or stopped become even less.

Think this seems a bit far-fetched? A few facts may provide some insight:

- The cost of cybercrime is now estimated to be greater than)the illegal drug trade and the fastest growing crime in the world, yielding US$114 billion [2].
- The President of the United States (Obama) announced the "cyber threat is one of the most serious… threats we face" [3]
- It's estimated there are 2 BILLION Internet users [4] – all able to knock on your "internet doorstep" every minute of every hour of every day. Even if only tiny portion – just 1% – is interested in compromising your online presence, that's 20 million people or almost the entire population of Australia.
- In 2011 there were more than 280,000 "phishing attacks" on the Internet (where criminals deceive users into providing their online account details, which are then used to commit online fraud). On average, each attack yielded US$4,500 for criminals – equating to more than US$1.26 billion [5].

[2] *"Norton Cybercrime Report" (Symantec)*
[3] *http://www.whitehouse.gov/cybersecurity/*
[4] *http://www.internetworldstats.com/*
[5] *"The Year in Phishing. January 2012" (RSA)*

Clearly, for a diversity of people and cultures across the globe the rewards from cybercrime are fruitful and may seem to many to be worth the risk of being caught.

Rethinking Security in the New Digital Frontier

Before exploring any new frontier, it's obviously important to understand the different conditions (e.g., weather, terrain, food supply) and rethink the assumptions in your plan.

Organisations leveraging today's Internet need to do the same, particularly when it comes to how they protect their and their customers' sensitive data from cyber threats. Here are some key things to think about.

- **"On the internet, nobody knows you're a dog"** [6]: In a traditional 'bricks and mortar' world, customers are identified by physical means (visually, photo ID, signatures etc.), but on the Internet, organisations don't know whose fingers (or paws!) are really on the keyboard at the other end of a transaction. The anonymity of the Internet means that 'identify theft' has become one of the fastest growing crimes in the world. It also means users are much more brazen to try things they wouldn't otherwise do knowing it is harder to track them. On the Internet, organisations need an effective way of knowing ('authenticating') who they are dealing with over their digital channels, particularly when handling sensitive data.

- **Bricks and mortar outlets don't need to deal with robots, but digital channels do:** A worrying trend on the Internet is the increasing use of 'web bots' or 'bot nets' (groups of web bots) to attack sites. If a human hacker wanted to try and guess someone else's password or to bring a site down by flooding it with unwanted traffic, they just wouldn't be able to type fast enough. But enlist a computer to do this? Or maybe even 'hijack' a bunch of them from other Internet users? Now we've got a match! Organisations need to be increasingly prepared to deal with such attacks in the way they design their digital channels and the types of monitoring and response techniques they deploy.

- **Slower runners make for an easier lunch:** An old joke used to say that "when in a group of people being chased by a bear, you don't need to be the fastest to outrun the bear, you just don't want to be the slowest!" Similarly, when on the Internet, organisations need to ensure their digital channels are not a 'soft target' (i.e. weakest security and anti-fraud measures). It isn't necessary to make your systems impenetrable. In fact, this would probably lock out most of your customers as well. But also beware of what organisations you compare yours with. If the value of the data and transactions you put online is worth it, criminals may well target you, even if your security is not the weakest. It's important to ask, "What can be exploited?" and compare security against sites that offer similar 'crime spoils'.

- **Don't make it complex for your customers (and simpler for criminals):** A common mistake in online security is using controls that are too complex or cumbersome for customers. For example, requiring passwords that are too hard to remember, using logon processes with too many steps or that are cumbersome (e.g. overusing 'CAPTCHA codes'). Overly complex user 'authentication' methods not only make it harder for legitimate customers but also create opportunities for criminals. For instance, hard to remember passwords can result in high volumes of users requesting resets via a call centre, creating opportunities for criminals to deceive call centre staff and accessing user account details (a technique known as 'social engineering'). To avoid these pitfalls, it is important for an organisation to select the right 'trust model' for its digital channels. A good 'trust model' provides simple, yet effective authentication of users in a way that suits their demographics, sophistication with IT and online habits (e.g. always mobile vs. usually online at home or work),

Are You Worth the Chase? A Simple Test

For many organisations, it's hard to tell whether their digital channels and online data are attractive to cyber criminals.

Some simple questions to get a quick indication of whether your organisation's digital channels might offer an attractive crime prize include;

1. Are you experiencing high volumes of online customers reverting back to other channels, such as physical branches or call centres? (Online channels might be too complex for your customers)

2. Are your online customers 'naïve' about threats from the Internet – e.g. would they click on an email link asking them to sign on to a site that looks like yours? (Potential exposure to phishing attacks)

3. Are you handling high volumes of user ID or password resets (wither online or via call centres)? (Logon process maybe too complex or could be due to 'social engineering' attacks)

4. Do you allow customers to identify themselves using a variety of different means (e.g. by using any one of user ID, name and address, email address, phone, etc.)? (More opportunities for criminals to assume the identify of customers)

5. Do you have high numbers of online customer accounts with similar or virtually identical details? (May indicate fictitious or duplicated customer registrations)

[6] *Peter Steiner (The New Yorker, July 1993)*

6. Are your digital channels most active outside of the times of day when you'd expect legitimate customers to be using them? (May indicate attacks occurring from users in other time zones and / or use of web bots)

Now, add together the number questions you answered with a 'Yes'. If you have sensitive data online (e.g. credit cards, customer details etc.), then double the number.

If you scored 2 or 4, then it may be worth considering a little further. If you scored more than 4, listen out … you might just hear the sound of Old Grizzly's footsteps getting closer! In all seriousness, in today's online world, it's critical for organisations to keep a watch out for the telltale signs of cybercrime.

A Case Study: A Rush to Recruit Online Customers

Here is an example (fictional, but adapted from real occurrences) of an organisation registering online customers with little focus on establishing and validating their true identities: great for quickly amassing online registrations, but not so great for knowing who they really are.

With a goal of reducing transaction costs, "Erebus Ltd", a discount book retailer, undertook a campaign to migrate its customers from its traditional chain of 'bricks and mortar' outlets to its new online store. To promote the change, whenever a customer entered an Erebus store, the sales assistant would offer to register them online and, as an incentive, the customer would receive a credit for future purchases.

Online registrations soared! The only problem though was that, because many customers were not very 'IT savvy' they often forgot their IDs and passwords and would return to the store or contact Erebus' call centre. Since Erebus had a strong service focus, staff would gladly help customers locate their forgotten IDs or reset passwords. Alternatively, if the old ID couldn't be found, they would happily set up a new one.

After several months, Erebus' financial controller was reviewing the company's accounts and noticed a 300% spike in customer credits issued compared to forecast. Further investigations revealed this was due to a huge surge in credits issued to online customers, even though overall sales were flat. Of even greater concern was that, when the online accounts were analysed, it was impossible to tell which belonged to legitimate customers and which didn't. It also appeared that many customers had registered multiple times, but with slightly varying details, just to claim the credits. Sorting out this mess would take Erebus many months, wipe out its earnings for a quarter and tarnish reputation with its customers as it attempted to claw back illegitimate credits.

The next time Erebus decided to launch an online service, it thought carefully about the threats it might face and how to effectively identify and authenticate its customers to prevent such a situation reoccurring.

Another Case Study: Security with the Best of Intentions

Here is an example of how online security controls that don't work well for customers may help 'open the door' for cyber criminals.

"Acme Ltd" decided that online security was now to be its #1 priority. It launched a campaign to advise all of its customers of its new security measures, including stronger password requirements and a new online facility to reset forgotten IDs and passwords. The campaign launch took place via a blanket email to all of its customers, which for their convenience included a link to the Acmes web site. When customers linked to the revamped site, they were asked to set a stronger password and enter a new 'secret question and answer' to be used if they forgot these details. Recognising that many of their customers may need assistance, the email also invited them to contact the call centre, which would assist them to locate their previously registered details and set up new ones.

The campaign appeared to be a resounding success; with "acme.com" showing record levels of visits to its security pages and a steady flow of call centre requests for assistance.

Sometime later, Acme's IT manager received a call from the head of customer service who was irate. For the third time that day, a customer had reported unauthorised purchases using their online account as well as at other online stores using the credit card details they had stored online with Acme. "How can this be? I thought we had IMPROVED our online security?"

Stunned, the IT manager called the affected customers herself to find out what was going on. After several discussions, she finally discovered the source of the frauds.

Immediately following the launch of their new security campaign, someone had carried out a series of calls to the centre to obtain email addresses of Acme's customers. They then copied Acme's launch email word for word (including logo and images) and sent it out to a large number of customers. This would not have been so bad, except that instead of linking to "Acme.com", the email directed customers to a fraudulent website that resembled Acme.com and asked customers to key in their IDs, passwords, and other details. The criminals then used these details to access customer accounts on Acme's site.

A full investigation found that a large proportion of Acme's customers were snared by this well planned 'phishing' attack. As many customers were new to the online world, they did not readily identify the scam.

As the value of frauds against Acme and other online retailers grew, credit card companies were forced to reissue many compromised cards and significant fines were imposed on Acme. Acme also needed to issue an embarrassing letter to its customers notifying them of the incident.

So What Should Organisations Do?

The good news is that there is a plethora of security tools, techniques and mechanisms that can be deployed to ensure your organisation is not the softest and most attractive target for cyber threats. However, choosing the right security (simple, cost-effective, doesn't treat your customers like criminals) can be a challenge.

Here are five practical steps that organisations can take to help steer them toward the right decisions for digital channels.

1. **Know what sensitive data is being captured and where it is stored:** Channels such as web sites and mobile applications are great for capturing sensitive customer data – personal contact details, financial account information, medical histories and even tracking physical movements and locations. As more customer information is captured online services can become more personalised and targeted – but the value to cyber criminals also increases. The first step in protecting this data is to know what is being captured, through which channels, and where it is stored. This is also a critical step to ensure that privacy laws and regulations are being complied with.

2. **Test for security vulnerabilities:** Conducting an online "Penetration Test" (aka Pen Test) involves having someone scan or even attempt to hack into your systems using similar tools and techniques to a hacker. The idea is that by finding vulnerabilities before hackers do, organisations can mitigate them and keep themselves off a prospective hacker's hit list. As technologies and hacking techniques change frequently, it's often a good idea to conduct Pen Tests on a regular basis, such as annually for systems dealing with sensitive data.

3. **Examine digital channels through the lens of a criminal:** Plugging technical vulnerabilities is a good initial step, but determined cyber criminals won't just stop there – they'll also exploit weaknesses in an organisation's processes and procedures as well ask the 'human factor' using deception techniques (social engineering, phishing etc.). By conducting an online Threat Risk Assessment (TRA), organisations can 'put themselves into the shoes of a criminal' and determine how susceptible they are to cyber attacks, what the most likely paths of attack are, as well as which security measures (people, process, technologies, awareness) would best address any soft targets.

4. **Review online 'trust models':** An organisation needs to ensure their methods of identifying, authenticating and establishing 'trust' with their online customers are not only secure, but are well aligned with customer demographics, preferences and habits. Periodically reviewing alignment of these 'trust models' ensures the right balance of security and customer convenience. There may also be opportunities to simplify and streamline these processes – improving efficiency and the overall customer online experience.

5. **Keep on top of external service providers:** In today's world of outsourcing, offshoring, and cloud computing it is hard to find an organisation that doesn't use external IT service providers. While external service providers can take on service delivery responsibilities, risks of fraud, privacy breaches and reputational damage can't be outsourced. External service providers can also be a source of risk with their personnel and operations often geographically dispersed and 'out of sight'. Issues of legal jurisdiction should be considered if providers or their services are not based within locally. Clear security requirements in service provider contracts are crucial and, where sensitive data is involved, there should be mechanisms in place (e.g. right to audit) to ensure these requirements are complied with.

The Bottom Line: Keeping Your Organisation Out of the Headlines

Cyber-attacks have now moved from the 'tech pages' to mainstream media. Every week it seems there is a new cyber attack in the headlines. First there was WikiLeaks. Then came SONY (whose expenses exceed US$171 Million so far) and, locally, what about Vodafone or Telstra (major reputational damage) and Distribute IT (which cost its entire online business)?

The new reality is that, on top of the direct costs of cyber crime (fraud, service downtime, fines, lawsuits), the direct revenue impact on an organisation's reputation can be just as damaging. 26% of Australians said they wouldn't do business with a company if they knew it lost their personal details. [7] Even if you 'halve that estimate' to be conservative – how much would a loss of 13% to your revenue equate to?

In the new Digital Frontier, it's just not acceptable to assume that the methods of the past will still be valid or effective. It is also naïve for an organisation's management to think that their online services and data will be immune from cyber threat.

While customers and the public at large are demanding 'round the clock' access to data and services, they're also becoming increasingly intolerant of online privacy breaches. Getting the balance of service and security right is now a major challenge for organisations venturing onto the New Digital Frontier.

Keeping one step ahead of cyber criminals, however, does not always need to be difficult – it can be as simple as knowing what information is attractive to them and ensuring you're not a soft target.

[7] *Sail Point Market Pulse Survey 2011*

About TrustedImpact

Trusted**Impact** has a singular focus in Information Security. We help enterprises achieve their business objectives by protecting the flow of important information from unauthorised access, use, disclosure, disruption, modification, theft, or destruction.

Information security is all we do – we're specialists in information security, not part-time generalists who dabble in this complex discipline.

We use seasoned professionals with expertise in information security to position your organisation for growth and success. Our 'business driven context' means recommendations are practical; they reflect your business and integrate well into your day-to-day operations.

We're also independent consultants with no financial affiliation with technology vendors. This means our business model not about our success in reselling someone else's technology, but is purely focused on your success.

About the Author

Ron Speed is a seasoned security professional with 20 years of experience in operational and technology risk, information security, regulatory compliance, consulting, controls transformation and audit. He brings extensive "big 4" security consulting experience as well as International experience in the USA, Australia and with Asian regulatory requirements.

Ron is Certified in Risk and Information Systems Control (CRISC), a Certified Information Systems Auditor (CISA) and an active member of the Information Systems Audit and Control Association (ISACA) and the Cloud Security Alliance (CSA). He received a Bachelor of Information Systems from Monash University and is a Chartered Accountant from the Institute of Chartered Accountants of Australia.

Ron's a Principal Consultant with Trusted**Impact** and can be contacted on (03) 9023-9710 or via email at ron.speed@trustedimpact.com.