A game of Leap Frog Cyber Attacks and Cyber Security

an Interview with Kenrick Bagnall

In 2015 the top ten cyber scams earned criminals an estimated $1.2 billion from Canadian victims. Put another way, around 80,000 people unwittingly fall prey to these scams every day – equivalent to the population of Sarnia or Peterborough. The Toronto Police Services Computer Cyber Crime Unit, (C3) regularly hears and investigates cyber crimes that effect both individuals and corporations. Kenrick Bagnall with 20 years of corporate IT security expertise, currently a Detective Constable of the TPS Intelligence Services – Computer Cyber Crime Unit and a much sought after speaker on Cyber Security, kindly shared his expertise in this area. Below are Kenrick's great insights, account of current trends, and how to protect valuable assets and data both on an individual level and a corporate one.

TRENDS IN CYBER CRIMES

1. Cyber crime no longer just for the tech savvy

Once upon a time hackers needed to have a skill set that allowed them to perform cyber crimes. Now on the dark web with the rise of ransomware as a service, anyone can purchase ransom ware and execute the according scam. Similarly, distributed denial of service attacks are also available for purchase. This ease of access and affordability gives unethical business people new avenues to attack competitors and resourceful albeit misguided students the ability to hijack test servers to avoid writing an exam. On October 24, 2016, the Standardized Test service for Ontario High School Services test server was attacked. The Globe and Mail reported the cancellation of the Ontario Student literacy test caused by cyber attack, which affected 200,000 students.

2. Data being stolen is more than financial data

Once upon a time we all worried about bank account and credit card numbers being stolen. It seems that hackers have evolved and are now finding ways to monetize data such as Personal Identifiable Info (PII) and Personal Medical Info (PMI). The databases that are obtained find their way onto the dark web, and are sold using crypto currency.

HOW INDIVIDUALS AND CORPORATIONS CAN PROTECT THEMSELVES

A. INDIVIDUALS

1. Be protective of your email addresses

Most individuals are victims of random attacks. Using a more sophisticated password and increasing the strength and diversity of the password will protect you from Brute force attacks geared to attack an encrypted password. Intermix cases and use different characters in your passwords. Secondly, use multiple email addresses. Set one up for each use e.g. one for family and friends, one for subscriptions, one for teams. Remember, complex passwords are secure; long passwords are more secure.

2. Stay informed

As with any challenge, being informed gives you the power and the knowledge to protect yourself. Sites such as staysafeonline.org, cctx.ca are great sites to keep on top of how to protect yourself from cyber crime. According to the Norton Symantec Report on Cyber Crime, millenials and seniors are the groups most impacted by scams, each for different reasons. With the Millenials, this group doesn't see the issue of cyber security as a shared responsibility between themselves, corporations and government. They also do not have secure passwords and they share their devices. With seniors, lack of awareness of traditional fraud scams seems to be the biggest culprit.

3. Report it

Kenrick would like to see one stat increase, and that is the number of cyber attacks being reported to law enforcement by both individuals and organizations. Laws are being broken, crimes are happening, offences have real victims. These matters must be investigated.

B. ORGANIZATIONS

Every organization is vulnerable, and every system can be hacked. Organizations that have large volumes of PII and PMI and low budgets for network infrastructure and cyber security, and are essential services are targets. Numerous

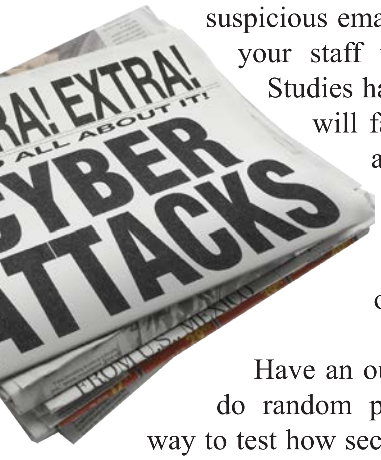
incidents are reported from education and healthcare institutions; there's a larger amount not being reported. Organizations involved in financial data are being targeted on a daily basis.

1. BC/DR Plans that include Cyber Incident Report component

Have a layered approach to security, firewalls and anti-virus is not enough, a more sophisticated security model is currently required. Your BC/DR plan should include a Cyber Incident Response component that addresses issues like:

a) How are you going to engage internal IT
b) What is the direct line to outsourced resources
c) How will you engage law enforcement

2. Train your staff on cyber awareness – use Random Penetration and Social Engineering Testing



Internal staff is often identified as the weakest link in cyber security. Train your people to know what a suspicious email or website looks like. Educate your staff through an awareness program. Studies have shown that up to 80% of staff will fall prey to a cyber attack, pre an awareness program, but only 30% of the same staff are vulnerable post an awareness program. If your people are more aware, your organization is more secure.

Have an outside cyber security organization do random penetration testing. It is a great way to test how secure your data is; how secure your infrastructure is and your people.

A random parking lot USB drop has been shown to be a successful way to infiltrate organizations. Hackers drop USBs in the parking lot of your offices, your staff pick them up and use them.

3. Back up your stuff and check restoring it on a regular basis

Your backup is only as good as the last time you checked restoring it. Test your restores. It is critical you have this plan ahead of time. You don't want to make decisions on the fly. During an incident you are going to be focused on getting up and running, not securing critical digital evidence and contacting law enforcement.

4. Understand what normal looks like

Cyber security is only going to pay off with reporting. When you understand what normal looks like you will recognize a yellow flag before it becomes a red flag. You will be able to report an online fraud to police and proactively provide investigators with meta data to assist with the investigation and have a much better chance of a positive outcome for the organization.

Understand what normal looks like in your organizations:

a) Normal traffic on the network
b) Normal traffic on the firewall
c) Normal in terms of staff activity and behaviour

LEAPFROG EFFECT

For every 10 foot wall of cyber security, there is a hacker building an 11 ft. ladder. Technology is evolving and is available both to cyber criminals and corporations, private sector and law enforcement. The good guys are using technology for good and the bad guys are using it for bad.

OUR JUDICIAL SYSTEM

Law enforcement can only enforce laws that are on the books. The Judicial system needs to keep up with the increasing threats and levels of attacks. We want to create good case law to promote a safe online environment. It is where people are working, taking part in commerce and communicating.

Definition of the Internet, Ontario Case of Appeals, 2012 R vs. Ward.

Kenrick is a contributor to Canadian Security Magazine where he has written several columns on Cybersecurity including cyber bullying and threats to critical infrastructure. Kenrick has been a keynote speaker and presenter on Cybersecurity at the Converged Security Summit (Atlanta, GA), The Fraud & Breach Prevention Summit (Toronto, ON), The Niagara Counterfeit and Fraud Workshop (Niagara Falls, ON), The Axis Communications USA Partner Summit (Tucson, AZ) and several other public sector and private industry symposiums.

Kenrick's background in Information Technology combined with his Law Enforcement experience has uniquely positioned him as an investigator, instructor and presenter on technology, information security and cyber investigations.

Article written by Vickie Gougoulias, Editor DRIE Digest ■