



DIGITAL DEFENCE - COMPLETE SECURITY BREACH PROTECTION



Cyber Security Breakout Session

Investment Industry Regulatory Organization of Canada, IIROC
02 December 2014

The Criminals are Winning – Why?

1. Physical (in)security
2. Social engineering
3. Indirect access
4. Insider threat
5. Vulnerabilities, patches and upgrades, exploits!
6. You're not prepared

Physical (In)Security

- “If I can boot, I can root” ...
- Physical security usually a “facilities problem”
- Walk fast; carry a clipboard (and yes, I DO have a work order)
- Dress all in brown, carry some packages – who am I?



Social Engineering

- 100% success rate
- Used on its own, or to facilitate attack
- Dumpster diving
- Shoulder surfing
- Call the phone centre / help desk (HBGary)
- “Please click this link”
- Road apples



Indirect Access

- Before an attack, hackers conduct reconnaissance to find weak link
- Mergers, acquisitions
- Partners - 3rd parties with authorized access to the network (Target, Home Depot!)
- Remote users
- Lost devices (laptops, smartphones, USB drive)

Insider Threat

- Accidents, leakage (Gmail anyone?)
- Sabotage
- Inappropriate use:
 - Time theft
 - Copyrighted material
 - Install malware
- Theft of resources + resale online
- Steal corporate data to sell, start own business



Vulnerabilities, Patches, Upgrades, Exploits

- Are all patches and upgrades applied?
- Failure of automated tools
- Default passwords
- Defender's dilemma:
 - Defender must protect everything
 - Attacker only has to find one opening ...
 - Troy, Masada, Maginot Line – how's that static defence working for you?



You're Not Prepared

- You're going to get hacked (not "if")
- Show of hands: how many of you have a documented incident response plan?
 - Is it pre-approved by management?
 - Has it been tested?
 - Does your business support the plan? Can it?
- Are you leveraging "response" or "management"?
- Is your first line of defence prepared?

DigitalDefence (www.digitaldefence.ca)

- Specialize in penetration testing, incident response, data forensics
- Training provider

Robert W. Beggs, CISSP

- 15+ years experience in all aspects of data security

The screenshot shows the Digital Defence website homepage. At the top, there is a navigation bar with links for Home, Advise, Protect, Respond, Training, Resources, Company, Contact, and RSS. Below this is a large banner with the heading "Have You Been Hacked?" and a sub-heading "If you think that you've suffered a security or privacy breach of your data, advice and complete 24x7 support is available from DigitalDefence." A "LEARN MORE" link is present. Below the banner are four service icons: Advise (Energy security & liability), Protect (Identify & prevent risks), Respond (Rapid security incident response), and Contact Us (Contact Digital Defence). The main content area features a "Cybercrime Specialists" section with a photo of two professionals and a list of services. To the right is an "Announcements" section with two news items. The footer contains a grid of service categories and contact information.

Contact Me

DIGITAL DEFENCE

Robert W. Beggs CISSP CISA

robert.beggs@digitaldefence.ca

tel (905) 681-3310

(866) 677-1337

cel (647) 444-1492

302 - 3310 South Service Road · Burlington · Ontario · L7N 3M6