# Integrating Cyber Insurance into your Cyber Security Arsenal

François Carrière Serguei A. Mokhov[1]

Concordia University
Gina Cody School of Engineering and Computer Science
Concordia University, Montréal, Québec, Canada
nag@encs.concordia.ca

Metricon X, 2019

[1] presenter, serguei.mokhov@concordia.ca

Université Concordia University

# Dr. Serguei A. Mokhov

**AITS, Security Research Center, NCFTA Canada, Concordia 3D Graphics Group, S4 Lab, Software Engineering Research Center**

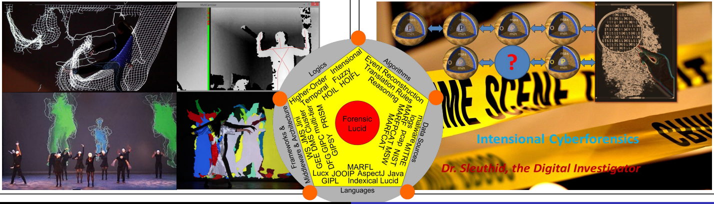
**Departments and groups affiliated with:** **Computer Science and Software Engineering, Concordia Institute for Information Systems Engineering, AITS, mDreams Stage Research Creation Group and CCIFF.ca, GIPSY R&D Group**

**Research expertise:** **HCI, computer and network security, formal methods, software architecture, refactoring, continuous integration, web services, AI and machine learning, graphics techniques, motion capture, multidisciplinary research and creation**

## Projects and Research Areas

- **Illimitable Space System** v2 and v3, **OpenISS**
  - continuous integration and refactoring
  - HCI, AR/VR/MR, CG, music visualization
  - motion capture, computer vision, signal processing
  - Max/MSP, Processing, OpenCV, OpenGL
  - working with artists and software engineers

- **Forensic Lucid**, Intensional Cyberforensics and **GIPSY**
  - Formal Methods, Compilers, Distributed Systems, Web Services
- **MARFCAT, MARFPCAT, OCTMARF**
  - Machine learning, AI, signal processing, code vulnerability and malware packet analysis



# Introduction I

As IT practitioners we can take all the precautions necessary for a safe and secure environment and still fail to keep unwanted intruders out.
In these instances a new trend in insurance has become available.
This presentation looks at the role of cyber insurance and its place in our security environment.

# Introduction II

You have been diligent [Wik13] and have installed the latest firewall, intrusion detection, anti-virus, anti-malware, spam filtering, e-mail and web browser protection.
You have optimized the file access, backup and patching procedures and updated the authentication, encryption and password policies so "What could possibly go wrong"? Well, anything and, unfortunately, everything.

# Factors I

As Donald Rumsfeld so eloquently put it:

> *"there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know." [Rum12]*

# Factors II

The “known knowns” [Rum12] are the easiest to identify and defend against.

Virus signatures, vulnerable protocols or susceptible applications all either have software fixes or patches available to correct the deficiencies.

These should be taken care of as quickly as possible in order to avoid being vulnerable to known exploits.

# Factors III

In the recent past, June 2017, NotPetya attack [Gre18] the A.P. Møller-Maersk corporation as well as other multi-national corporations' computer systems were subverted when Russian hackers combined the Mimikatz [MS16] vulnerability and the EternalBlue [Che16] penetration tool.

- Mimikatz was developed by Benjamin Delpy in 2011 and methods to limit its effectiveness were available soon after [Mic14].
- EternalBlue on the other hand was allegedly developed by the NSA and leaked to the public in April of 2017. Microsoft released the patch [Mic17] for EternalBlue in March of 2017.

# Factors IV

The information and tools needed to thwart this attack were available prior to the assault and yet this single incident caused 300 million dollars in losses to Maersk [Eco19] and over 10 billion dollars to the world economy as confirmed by former Homeland Security adviser Tom Bossert [Gre18].

# Unknown I

The "known unknowns" [Rum12] are events we know exist but do not know their nature or when, and if, they will strike.

Zero-day exploits are errors in the code for either software or hardware that are undiscovered by the developer and unknown to the end user.

# Unknown II

Such an error occurred in the OpenSSL code when Dr. Robin Seggelmann, introduced a programming error that inadvertently that lead to the "Heartbleed exploit" [Syn14].

> *"In one of the new features, unfortunately, I missed validating a variable containing a length", went undetected by the code reviewers and everyone else for over two years." [Moh14]*

# Unknown III

The code in the encryption library of the popular protocol had a flaw that was introduced as early as 2012 but the bug was not found until early April 2014 and a patch became available about one week later. No one will admit if the exploit was truly unknown before then.
"Shellshock" affecting `bash` was another one, took even longer...

# Unknown IV

Finding these vulnerabilities and developing toolkits to use the results has lead to a market that continues to flourish.
From cybercriminals, large corporations and government institutions the search for and acquisition of zero-day exploits is an active lucrative endeavour.
Table 1 is from a Forbes magazine article from 2012 and high lights the availability of exploits [Gre12].

# Unknown V

Table: Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits [Gre12]

| Software | Cost |
|---|---|
| Adobe Reader | \$5000–\$30000 |
| Mac OS X | \$20000–\$50000 |
| Android | \$30000–\$60000 |
| Flash or Java Browser plug-ins | \$40000–\$100000 |
| Microsoft Word | \$50000–\$100000 |
| Microsoft Windows | \$60000–\$120000 |
| Firefox or Safari | \$60000–\$150000 |
| Chrome or Internet Explorer | \$80000–\$200000 |
| IOS | \$100000–\$250000 |

# Unknown VI

While these are more difficult to counter the industry has been developing heuristic tools to detect abnormal activities and behaviours that help identify the source of the problem and allows the security team to decide on their next step.
These tools provide a vast array of powerful defense capabilities, but are not perfect (we can refer to next-gen firewalls and appliances such as produced by Fortinet, Checkpoint, Cisco and others or even AI-enabled platforms that adapt dynamically to network traffic, such as Darktrace or Vectra Networks).

# IoT I

Then, of course, there are the “unknown unknowns” [Rum12], the things that until they are discovered are not in our plans.

Recently the rapid growth and adoption of the Internet-of-Things and the latest trend towards bringing your own device to the office have introduced new challenges to our cyber defenses.

Who would have considered that a new refrigerator, a smart watch or an automatic lighting system could pose a threat to our information system and data?

# IoT II

These devices do not need human intervention to find other devices to communicate and share data with.

They sit collecting information, maintaining communication with other devices or the internet waiting for further instructions.

Hackers can use these insecure devices to access the company's network or they may also use a combination of devices and launch a DDoS attack.

For situation such as these we can only hope that our staff and systems are resilient enough to withstand the attack and recover quickly.

The largest 2016 DDoS on "Krebs on Security" with the Internet-enabled cameras is an example of that.

# IoT III

*"You could spend a fortune purchasing technology and services, and your network infrastructure could still remain vulnerable to old-fashioned manipulation. –Kevin Mitnick" [Mit18]*

# Enter the Humans I

In today’s business world no one has the time to wait.
We are continually connected to our workplace through all kinds of electronic devices and are often expected to be available 24/7.
We can and do train our users about cyber security awareness knowing that they often hear, but do not listen to the pitfalls.
We often hear “I don’t have time for updates’, “I can’t remember passwords for every account, so I use the same one” or “I brought my computer home and my kids must have used it”.

# Enter the Humans II

Classic social engineering, phishing, spear phishing and whaling, that persistent Nigerian prince with promises of millions, your bank with an account error to correct or your tax collection agency looking for your banking information to accelerated your tax refund are abundant.
All of these seemingly simple techniques would have been abandoned long ago if it were not for their effectiveness.

# Enter the Humans III

Even though we have setup up our cyber defence policies, procedures, and appliances are all in place the cyber antagonist relies human nature knowing that our biggest vulnerability is the user.

> *"Human behavior, or Layer 8 of the OSI model, or the iD10T error, or "the problem is obviously between the chair and the keyboard" type humor not only highlights the frustrations but also the greatest and most difficult to control vulnerability, the human mind." [Sma11]*

# Training I

Training the users was once considered an effective method of raising cyber security awareness and an act of due diligence on behalf of the organizations.

However, the complete validity of this statement may be questionable due to the number of successful attempts made by outsiders to access secured systems.

# Training II

In a survey by the SANS institute,

- “74 percent of the threats entered as an email attachment or link,
- 48 percent entered the browser via web-based drive-by or download, and
- 30 percent through application vulnerabilities on user endpoints.” [Nee17]

# Training III

More critique comes from a recent article on CSO titled “Does security awareness training even work?” [Kor15] If even well-educated security experts mess up when it comes to security, can we really adequately educate average employees to be more security aware?

# Training IV

Even though the training may not be adequate and like most training should not be considered “fire and forget”.
There are continually new methods developed by hackers to get in the systems and users need to be continually training against these new methods.
Reminders, testing and simulations can be used to reinforce what was learned but are not a guarantee and may not cover the newer methods used by the hackers.
All of this training can also be a burden both in time and money.

# Regulation I

The relationship between cyber-attackers and defenders has been in constant flux for several decades.

For every new method developed to get into the computer a new method was developed to thwart the attack.

What has changed that made cyber-insurance an interesting option now.

# Regulation II

Mainly new government regulations

- in Europe, the General Data Protection Regulation (GDPR) [Eur18] introduced in May 2018,
- in Canada the The Personal Information Protection and Electronic Documents Act (PIPEDA) [Can18] introduced in November, 2018 and
- California the California Consumer Privacy Act of 2018, [Cal18]

# Regulation III

- as well as each individual State's and or economic sectors privacy regulations such as:
  - Family Educational Rights and Privacy Act (FERPA), 1974
  - The Health Insurance Portability and Accountability Act (HIPAA), 1996
  - Children's Online Privacy Protection Act (COPPA), 1998

# Regulation IV

These new regulations placed the onus of protecting the information stored on the company's network on the company with financial implications for data breaches.
Understanding the scope and navigating the can be an odious task and should not fall on the shoulders of the it staff they have enough on their plate just managing the machines.

# Insurance I

Cyber insurance is still a relatively new concept in Canada, but the companies that provide insurance are introducing new products that cover the many different types of cyber incursions and their consequences.

# Insurance II

We surveyed 16 insurance companies in Canada for any presence of the cyber security insurance through their public information on their web sites and reaching out with email. At the time of writing this article, very few got back to us.

# Insurance III

| Insurer (active in Canada) | Cybersecurity Insurance |
|---|---|
| All State Insurance Canada | None |
| Largerst Canadian owned insurance business Cooperators | None |
| Desjardins | None |
| Federated Insurance | ** Have articles about it. Provide insurance? Not sure. |
| Great American Insurance | ** Cyber risk insurance. |
| Great West | None |
| Intact | None |
| Lloyds | ?? appears to be in the members only area |
| Manulife | None |
| Sunlife Insurance | None |
| TD insurance | None |
| The Personal Insurance | None |
| Wawanesa | None |
| Travellers | ** Yes |
| AIG | ** Yes |
| Zorich | ** Yes |

# General Coverage I

Type of incidents that can be covered

Cyber and Privacy Liability

- Business Interruption
- Court Attendance compensation
- Electronic data breach
- Electronic media liability
- Public Relations services
- Regulatory Investigation and Fines
- System and Data restoration costs
- Virus & Hacking liability

# Coverage First Party I

Cyber and Privacy First Party Loss:

- Privacy breach notification and Mitigation costs
  - Privacy liability for failure to prevent unauthorized access
  - disclosure
  - collection of confidential information
  - failure by others to whom such information was entrusted.
- Cyber Extortion
- Cyber Theft
- Cyber Crime with Electronic Social Engineering
- Forensic Investigation Expense: Covers the costs for forensic experts to determine how the intruder got into the device/system and what data have been compromised.

# Coverage First Party II

- Network Security Liability for a failure of network and computer systems' security to prevent or mitigate the impact of a cyber event.
- Reputational loss: Business interruption due to loss of trust in the wake of a cyber event
- Internet of Things (IoT) coverage for negligence in the design or manufacture of an IoT product and/or service.

# Coverage Third Party I

- Privacy Infringement Liability (Third Party)
- Media liability for online libel, slander, disparagement, misappropriation of name or likeness, plagiarism, and trademark and copyright infringement.
- Notification Recipient Services: Covers the cost in providing fraud remediation services to individuals that have been affected by the breach.

# Other I

## Advantages

- Insurers install the hardware, software, and provide maintenance services for the insured to be in conformance with the due diligence law [Wik13] (e.g., in the small coffee shop franchises offering free Internet access)
- Insurance can be issued from individual households, to small and medium businesses, that are more likely than not to have the capabilities and knowledge to adequately protect themselves
- They provide adequate training to the local staff or offer cloud monitoring of the same by a trusted 3rd party vendor

# Other II

- Small, startup, and medium businesses.
- Metrics community – standards and metrics can be used as an input.

# Other III

## Limitations

- Privacy breaches insurance – what does it really provide on the moral and other grounds to the victims whose PI was stolen via an unencrypted laptop (or even as was recently demonstrated with encrypted devices as well as long as its in physical possession of the attacker), or inadequate perimeter defences or lack of proper resources to monitor them for the likes of Target, Ashley Maddison, Equifax, and others?
- By offering cybersecurity insurance policies, would the insured become more "lazy" and "lax" in their digital security habits?
- "Cybersecurity is not important‘‘ [Odl19]?...

# Other IV

- We are not offering a ready-made solution for insurers or their potential clients and do not connect with any related actuarial machinery.
- Convincing insurance companies to offer cybersecurity insurance as a profitable entreprize.

# Future/Ongoing Work I

As we are collecting more data from the insurance companies, we refine the cyber threat insurance categories. We plan to extend this with an attempt to quantify reasonable bounds for the costs for the cyber insurance providers and consumers based on the security debt and other related metrics.
Important questions arise:

- How do you monetize these types of incident insurance coverage items?
- What need to be in place so you can be covered?
- What actions are taken if there is a breach? (Given that there were recently many so high profile breaches).

# Future/Ongoing Work II

- Deductables and Premiums? Smaller businesses that could afford insurance better than a full out security infrastructure with the onsite provided security devices, configuration and training by a qualified insurer and/or their subcontractors.

# Conclusion I

This and other body of work and facts have demonstrated that regardless of what defenses we place before potential attackers eventually one will get into our system the the consequences may be economically devastating.

Cyber insurance can provide the necessary after incident response by replacing articles if any physical damage incurred, control any fiscal implications and restore consumer confidence into the business.

For these reasons cyber insurance should be included in cyber security practice.

# Acknowledgment

- This work is supported by the Gina Cody School of Engineering and Computer Science, Concordia University, Montreal, QC, Canada.

# Questions? Discussions...

Thank you :-)

# Definitions I

Here we define some commonly known terms as used in this paper.

First party insurance Type of insurance policy under which an insured (the first party) is paid by his or her insurer (the second party) in the event of an accident, injury, or loss whether caused by itself or someone else (the third party).

# Definitions II

Liability insurance purchased by an insured (the first party) from an insurer (the second party) for protection against the claims of another (the third) party.

# Definitions III

Phishing is a general term for e-mails, text messages and websites fabricated and sent by criminals and designed to look like they come from well-known and trusted businesses, financial institutions and government agencies in an attempt to collect personal, financial and sensitive information. It's also known as brand spoofing [Roy15].

# Definitions IV

Spear-phishing is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons. This is achieved by acquiring personal details on the victim such as their friends, hometown, employer, locations they frequent, and what they have recently bought online. The attackers then disguise themselves as a trustworthy friend or entity to acquire sensitive information, typically through email or other online messaging [Gia18].

# Definitions V

A whaling attack is a targeted attempt to steal sensitive information from a company such as financial information or personal details about employees, typically for malicious reasons. A whaling attack specifically targets senior management that hold power in companies, such as the CEO, CFO, or other executives who have complete access to sensitive data. Called "whaling" because of the size of the targets relative to those of typical phishing attacks, "whales" are carefully chosen because of their authority and access within the company. The goal of a whaling attack is to trick an executive into revealing personal or corporate data, often through email and website spoofing [Gia17].

# References I

California State Legislature.
California consumer privacy act.
[online], KnowBe4, June 2018.
https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=Consumer+Privacy+Act+of+2018.

Canadian Parliament.
Personal information protection and electronic documents act.
[online], KnowBe4, November 2018.
https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/.

Check Point Research.
EternalBlue – everything there is to know.
[online], accessed Sept 11, 2018, February 2016.
https://research.checkpoint.com/eternalblue-everything-know/.

# References II

The Economist.
Black swans and fat tails. the market for cyber-insurance is growing.
*The Economist*, January 2019.
https://www.economist.com/finance-and-economics/2019/01/26/the-market-for-cyber-insurance-is-growing/.

European Union Parliament.
General data protection regulation.
[online], KnowBe4, May 2018.
https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr_en.

Nena Giandomenico.
What is a whaling attack? defining and identifying whaling attacks.
[online], Digital Guardian, July 2017.
https://digitalguardian.com/blog/what-whaling-attack-defining-and-identifying-whaling-attacks.

# References III

Nena Giandomenico.
What is spear-phishing? defining and differentiating spear-phishing from phishing.
[online], Digital Guardian, April 2018.
https://digitalguardian.com/blog/
what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phi

Andy Greenberg.
Shopping for zero-days: A price list for hackers' secret software exploits.
*Forbes*, March 2012.
https://www.forbes.com/sites/andygreenberg/2012/03/23/
shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits

Andy Greenberg.
The untold story of NotPetya, the most devastating cyberattack in history.
*WIRED*, August 2018.
https://www.wired.com/story/
notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

# References IV

Maria Korolov.
Does security awareness training even work?
[online], CSO, September 2015.
https://www.csoonline.com/article/2987822/data-protection/does-security-awareness-training-even-work.html.

Microsoft.
Microsoft security bulletin MS17-010  critical.
[online], May 2014.
https://docs.microsoft.com/en-us/security-updates/securityadvisories/2016/2871997.

Microsoft.
Microsoft security bulletin MS17-010  critical.
[online], March 2017.
https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010.

# References V

Kevin Mitnick.
Quote on company website.
[online], KnowBe4, September 2018.
https://www.knowbe4.com/about-us/.

Mohit Kumar.
Heartbleed bug explained - 10 most frequently asked questions.
[online], April 2014.
https://thehackernews.com/2014/04/heartbleed-bug-explained-10-most.html.

Jim Mulder and Mark Stingley.
Mimikatz overview, defenses and detection.
[online], SANS Institute reading room, February 2016.
http://www.sans.org/reading-room/whitepapers/forensics/mimikatz-overview-defenses-detection-36780.

# References VI

Lee Neely.
Defense in depth: An impractical strategy for a cyber world.
[online], SANS Institute, August 2017.
https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910.

Andrew Odlyzko.
Cybersecurity is not very important.
[online], revised March 18, 2019, March 2019.
http://www.dtc.umn.edu/~odlyzko/doc/cyberinsecurity.pdf.

Royal Canadian Mounted Police.
E-mail fraud / phishing.
[online], January 2015.
http://www.rcmp-grc.gc.ca/scams-fraudes/phishing-eng.htm.

# References VII

Donald H. Rumsfeld.
News transcript: DoD news briefing - Secretary Rumsfeld and Gen. Myers.
[online], news briefing, February 2012.
http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636.

Prescott E. Small.
Defense in depth: An impractical strategy for a cyber world.
[online], SANS Institute, November 2011.
https://www.sans.org/reading-room/whitepapers/warfare/defense-depth-impractical-strategy-cyber-world-33896.

Synopsys.
The heartbleed bug.
[online], April 2014.
http://heartbleed.com/.

# References VIII

Wiki Books.
Canadian criminal law/defences/due diligence.
[online], Wiki Books summary, October 2013.
https://en.wikibooks.org/wiki/Canadian_Criminal_Law/Defences/Due_Diligence.