

WOMEN'S INSURANCE NETWORKING GROUP



May 9, 2014

The background image shows a conference room with a large white oval table and several red chairs. The text "Welcome!" is overlaid on the image in large blue letters.

Welcome!

How Cyber Attacks are Changing the Way the Industry Manages Risks



In today's cyber world, everybody has been breached. In reality, it's more like continual breaches.

- Rick Betterley, President
Betterley Risk Consultants Inc.



Mary Gardner

- VP of Business Resilience, Zurich North America
- Spent 12 years with international insurance brokerages.
- Focus on crisis management, business recovery, IT Disaster Recovery and oversight of global sourcing partners.
- Served as Director of Business Risk for several major international companies.



Elisabeth Case

- SVP, Senior Advisory Specialist
National FINPRO, Marsh
- Works extensively with clients on
cyber and E&O programs.
- Spent five years previously at Marsh as a
placement specialist handling errors and
omissions, cyber, property, casualty and
international insurance programs.
- Served as Chief Underwriting Officer for the
Technology Industry Segment at CNA



Lauren Cisco

- AVP, Global Technology & Privacy Practice, Lockton Companies
- Served as a member of Aon's Professional Risk Solutions team.
- Specializes in crafting and securing risk transfer programs for information security and privacy, professional liability and media driven risks.
- Strategized and implemented Errors & Omissions and Security & Privacy liability insurance programs for global enterprise organizations



Guy Fuller

- President and Founder, Cybersavants, LLC
- Served as Director of Technology for Northwestern Mutual.
- Extensive experience in building technology teams charged with every aspect of IT ranging from security to application development.
- Spent 20 years concentrating on the information technology needs of healthcare and financial services companies.



Cyber Risk is a red hot topic. Do you have a perspective on the severity of the personal and business risk issues that we are facing?



CYBERATTACK!

Criminal hackers have assembled vast armies of hijacked computers

2003

The Slammer computer worm spread rapidly through the Internet, infecting approximately 75,000 computers in ten minutes. Regular Internet traffic slowed to a crawl, Web sites crashed, *ATMs failed, airline flights were grounded, and computer and safety systems at a nuclear power plant were disrupted.*

2007

A series of cyber attacks targeted Estonia, affecting the government, the media, and banks. Most of the attacks stemmed from hijacked computer networks (botnets), which caused more than one million computers in 75 countries to swamp their targets with bogus requests for information.

CYBERATTACK!

Criminal hackers have assembled vast armies of hijacked computers

*Computer worms are malicious programs that automatically copy themselves from computer to computer via the Internet. Like other types of malicious software, computer worms are usually assigned individual names, such as Slammer.

2010

The highly sophisticated Stuxnet computer *worm infected industrial-control systems at a nuclear plant in Iran.*

2014

John Mulligan, Target's chief financial officer, said the retailer was "deeply sorry" for a breach that affected both payment data of **40 million** customers and the *personal data, such as phone numbers and addresses, of as many as 70 million people.*



**If you were to
give a short
description of
Cyber Risk what
would it be?**

Cyber Risk:

Can also be thought of as
*Network Security &
Privacy Liability, or
Information Risk.*



It is liability due to harm suffered by others for **loss of their personal or corporate confidential information** in your care, custody, or control, and the costs your firm incurs to provide a breach response.



**What are your
clients asking for
in terms of
coverages and
advice as they
delve into this
issue?**

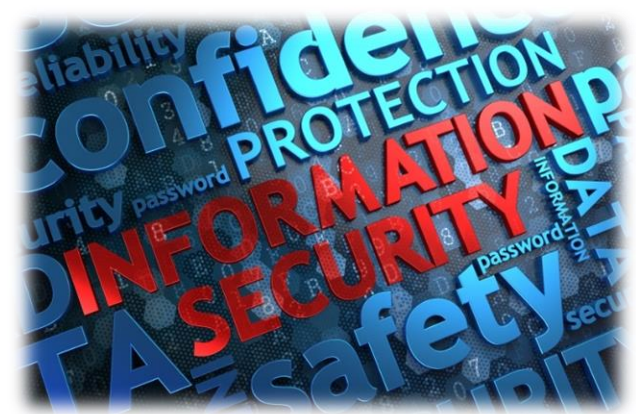


Cyber Insurance Coverages

Network Security Liability

Claim expenses and damages emanating from network and non-network security breaches

- Denial of service attack
- Transmission of a virus
- Theft of data



Privacy Liability

- Claim expenses and damages emanating from violation of a privacy tort, law, or regulation
- Claim expenses and damages emanating from a violation of a law or regulation arising out of a security breach



Payment Card Industry Fines and Penalties

Cyber Insurance Coverages

Privacy Event Expense Reimbursement

- Expense reimbursement for third-party forensics costs
- Public relations and Legal
- Mandatory notification costs (comply with security breach notification laws)
- Voluntary notification costs
- Credit monitoring
- Call center
- ID Theft Insurance



Privacy Regulatory Proceedings and Fines

- Claim expenses in connection with a privacy regulatory inquiry, investigation, or proceeding
- Privacy regulations fines & penalties



Breach Response Timeline

Breach is Discovered

Can be discovered internally

Can be discovered by trends in card fraud, financial institution monitoring, or government agency monitoring cyber space

*Target was notified by the Secret Service

Escalation to Insurer

Organize breach response team: forensics, counsel, insurer

Investigate incident to discover root cause

Possible data restoration

Determine population and scope

Prepare notice documents

Implement notification and call center assets

Notification

Establish crisis management response for media and public relations

Respond to requests from regulators

Provide credit monitoring service to affected population

Post Notification

Preclude and prevent litigation by preemptively notifying victims and rectifying security flaws

Insurer still supports in defense and litigation of claims

Identify opportunities to evolve security plan



What are corporations and Boards demanding in terms of Risk Mitigation and Business Continuity Planning?



Suggested Risk Mitigation Activities

Local risk: recommendations for individual organizations

Basic: regardless of the size of the organization, there is a relatively small set of actions to protect from most cyber risks

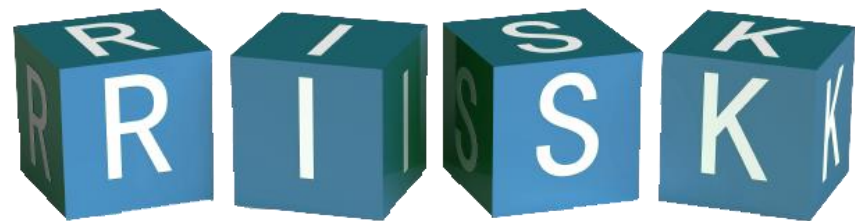
- Provide application whitelisting
- Use standard secure system configurations
- Patch application software within 48 hours
- Patch system software within 48 hours
- Reduce the number of users with administrative privileges

Advanced: larger, more sophisticated organizations should certainly implement the 20 Critical Security Controls, but they also have the capability to engage in far more advanced cyber risk management.

- Push out risk horizon
- Cyber insurance
- Demand more resilient and secure standards and products
- More effective board-level risk management

Resilience: for all organizations, and in some ways, perhaps the most effective.

- Redundancy
- Incident response and business continuity planning
- Scenario planning and exercises



**Let's get
personal.
What can we do
as individuals to
protect
ourselves?
What is your
best advice?**



PROTECT YOURSELF!

Remember that cyber insurance is corporate insurance, not personal insurance coverage, therefore, these suggestions are for corporate best practices, not individual things to do.



- Encrypt corporate portable devices, particularly laptops.
- Enforce a regular password refresh policy.
- Promptly disconnect employees from access to all corporate systems upon termination of employment.
- Only grant access to systems that employees require for their role.
- Require annual acknowledgement of corporate security policies and procedures and email and internet usage policies by all employees.



PROTECT YOURSELF!

- Install antivirus, spyware-detection, and firewall software on your computer. Keep that software and your operating system updated with all security updates.
- Think before you click on links or open attachments in e-mails or instant messages—even from friends. Be especially cautious if the mail is unsolicited and asks for personal information or passwords.
- Never copy or run software from unknown sources.
- Use passwords that have at least eight characters and include numbers and symbols, and change them regularly. Use different passwords for different accounts.
- Do business online only with reputable companies that use secure connections.*
- Do not give out confidential information about yourself or your accounts when using unsecured Wi-Fi connections, such as in public places.
- Switch your computer off when it is not in use.
- Regularly back up your files, and store copies securely.



*Do what you can to protect
your online security*



*** Secure Web pages on Web browsers display a lock symbol and https:// in the address bar. The "s" means secure.**

PROTECT YOURSELF!

- Passwords:
 - Complicated (numbers, characters, upper and lower case letters)
 - Don't always use the same one
 - Change often and definitely after a known incident
- Take action when you are notified of an incident
- Don't give away private information unless it is warranted (do they *really* need your social security number?)
- Be leery of hubs like airports with free Wi-Fi
- Check statements for fraudulent activity and inquire if you don't recognize a charge
 - Don't leave your laptop in your car or in a place where it can be easily taken
 - Use Find My Phone or other remote wiping options on your mobile device

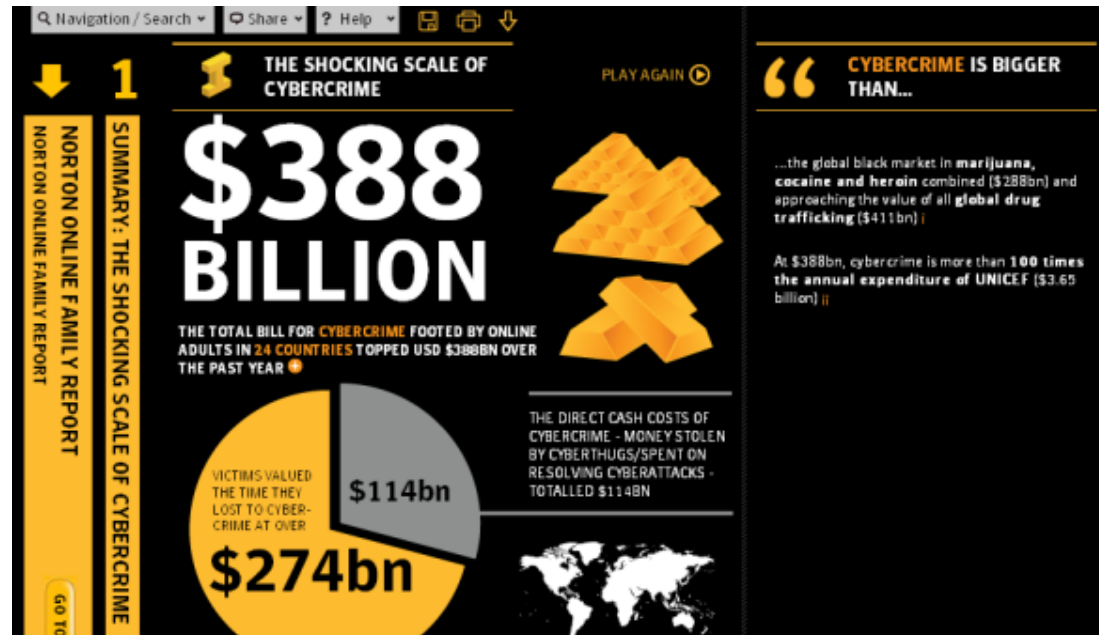


**The industry is
facing a number
of emerging
cyber trends.
What do you see
in your crystal
ball for the
future? What
should we be
watching out
for?**



Emerging Cyber Risk

According to Symantec, cyber crime is now bigger than the heroin, cocaine and marijuana markets combined!



- We live in a rapidly changing world!
 - New Technologies will present new exposures to loss
 - Business interruption
 - Terrorism, hacking, vandalism
- **How do you manage these risks?**



Emerging threats from a consumer perspective

Malware Will Be Cross Platform, Making Use of Novel Smartphone Features

New threats continue to target iPhone and Android users

Customers should install vendor software updates



May 2014 Chicago WING Luncheon

- Constantly evolving global privacy laws and regulations
- Big Data: implications of data gathering and expanding rights of consumers
- Beyond data security and privacy risks
 - Bodily injury and property damage caused by cyber attacks
 - Reputational harm (future lost business)
- Impact of social media
- Mobile device applications
- “The Cloud”
- Bring Your Own Device (BYOD)



Thank you!

Special thanks to our moderator Mary Gardner and our panelists Elisabeth Case, Lauren Cisco and Guy Fuller.

Thank you to Chubb for hosting!

See you in the fall!

Be sure to join the Women's Insurance Networking Group (WING) on LinkedIn



JACOBSON