Cybercrime, Digital Evidence and the Impact on an Intellectual Property Practice

Mitch M. Gilfillan
309.674.1133
Mgilfilln@quinnjohnston.com

What is Cybercrime?

- Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense.

- Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitive or malicious purposes.

- Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers.

Cybercrime, Black's Law Dictionary (10th ed. 2014).

What are different types of Cybercrime?

- Online banking;
- Identity Theft;
- Online Predatory Crimes;
- Virus attacks and spam; and
- Unauthorized computer access, to name a few.

Places Where Cybercrime most-often committed?

- Workplace computers;
- Networks and other online databases;
- Information technology (IT) resources; and
- Homes.

-USA Today


THREAT Toons™
by: Alex Savchuk
ALL OF OUR CYBERSECURITY ISSUES HAVE BEEN SOLVED WITH ZERO EFFORT AND MINIMAL BUDGET...
APRIL FOOLS'!!!
Is your CSO playing April Fools' jokes?

Cybercriminals in the Workplace: What to do?

- Failure to take appropriate precautions exposes the enterprise to otherwise avoidable or manageable risks and fallout.
- Evidence of criminal activity may be a potential violation of federal or state obstruction of justice statutes.
- Duty to report? Evidence of child-related issues.
- Although such offenses require proof of criminal intent associated with the destruction of evidence, the government may not share your view when it comes to the existence of that intent.
- Destroying, purging and emptying ("trash bin") evidence
    - Be careful - 720 ILCS 5/11-20.1(b)(5)

Execution of a Search Warrant, Subpoena or Request to Search

Steps when law enforcement suspects criminal activity:

- What to do?
- Contact attorney for advice
- Probable cause for a search warrant?
- Privacy issues?
- Notice issues?
- Do you have a response plan in place?
- Who has responsibility for managing the situation?

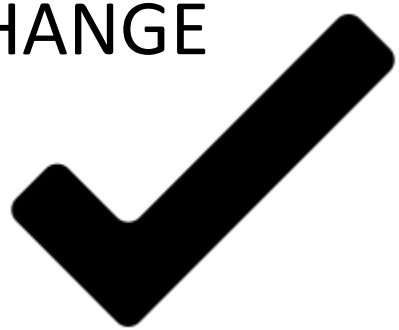
What to do if you suspect an employee of criminal activity?

At some point, everyone will face some level of criminal activity in the workplace:

- Should the employee be confronted?
- Should additional investigative work be undertaken?
- Should law enforcement be called?
- Is there a duty to report this activity to law enforcement?
- Can steps be taken to control the impact?
- How to/who will handle public relations?

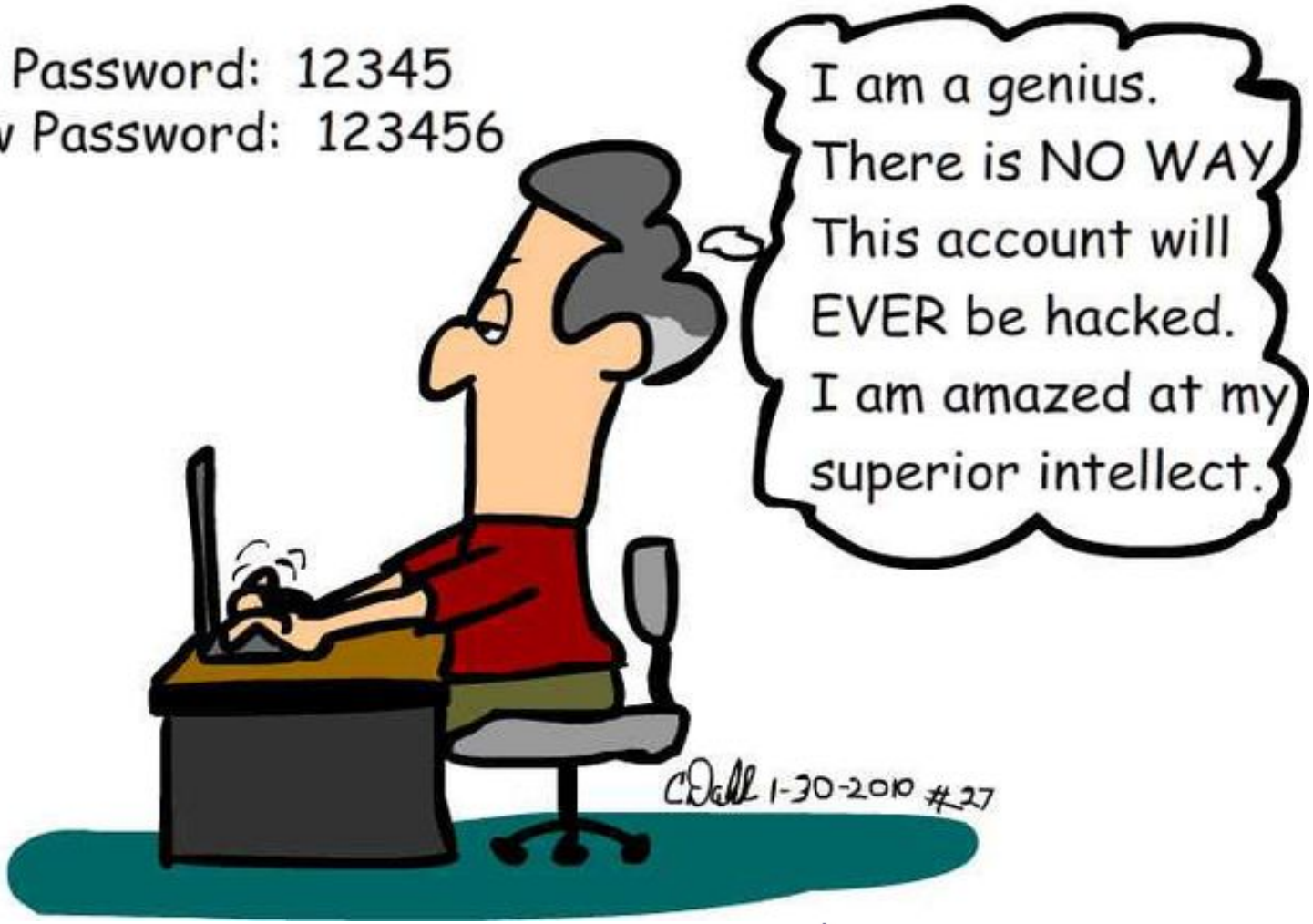
Steps to Prevent Cybercrime in the Workplace

1. Firewalls
2. Antivirus software
3. Encryption/cryptography
4. Access restriction and passwords – CHANGE OUR PASSWORDS!
5. Cameras
6. Locks/access devices
7. Controlled use of removable and portable devices (e.g., thumb drives, cell cameras) – policy in place?



[For Security Purposes, You Must Reset Your Password]

Enter Old Password: 12345
Enter New Password: 123456



Illinois Computer Crime Laws

Illinois computer crime laws differentiate between misdemeanor computer crimes (sending spam, for instance) and felony computer crimes (such as financial fraud).

Illinois Computer Crime Prevention Law (1987)

One way the state battles computer crimes is through the Illinois "Computer Crime Prevention Law" (ICCPL), which makes unauthorized computer use a criminal offense. The law is broken down into three (3) major categories:

1) Computer Tampering: This includes gaining access to a computer, a program, or data, without permission from the owner and creating or distributing computer viruses.
2) Aggravated Computer Tampering: This crime pertains to the government specifically. You can be in violation of the law if you tamper with a computer and you have the intended effect of: (a) disruption of or interference with vital services or operations of State or local government or a public utility, or (b) creating a strong probability of death or great bodily harm to other individuals.
3) Computer Fraud: This crime pertains specifically to using a computer for fraudulent activities.

720 1LCS 5/16D-1, 720 1LCS 5/17-50 et seq.

Cyber Liability Insurance

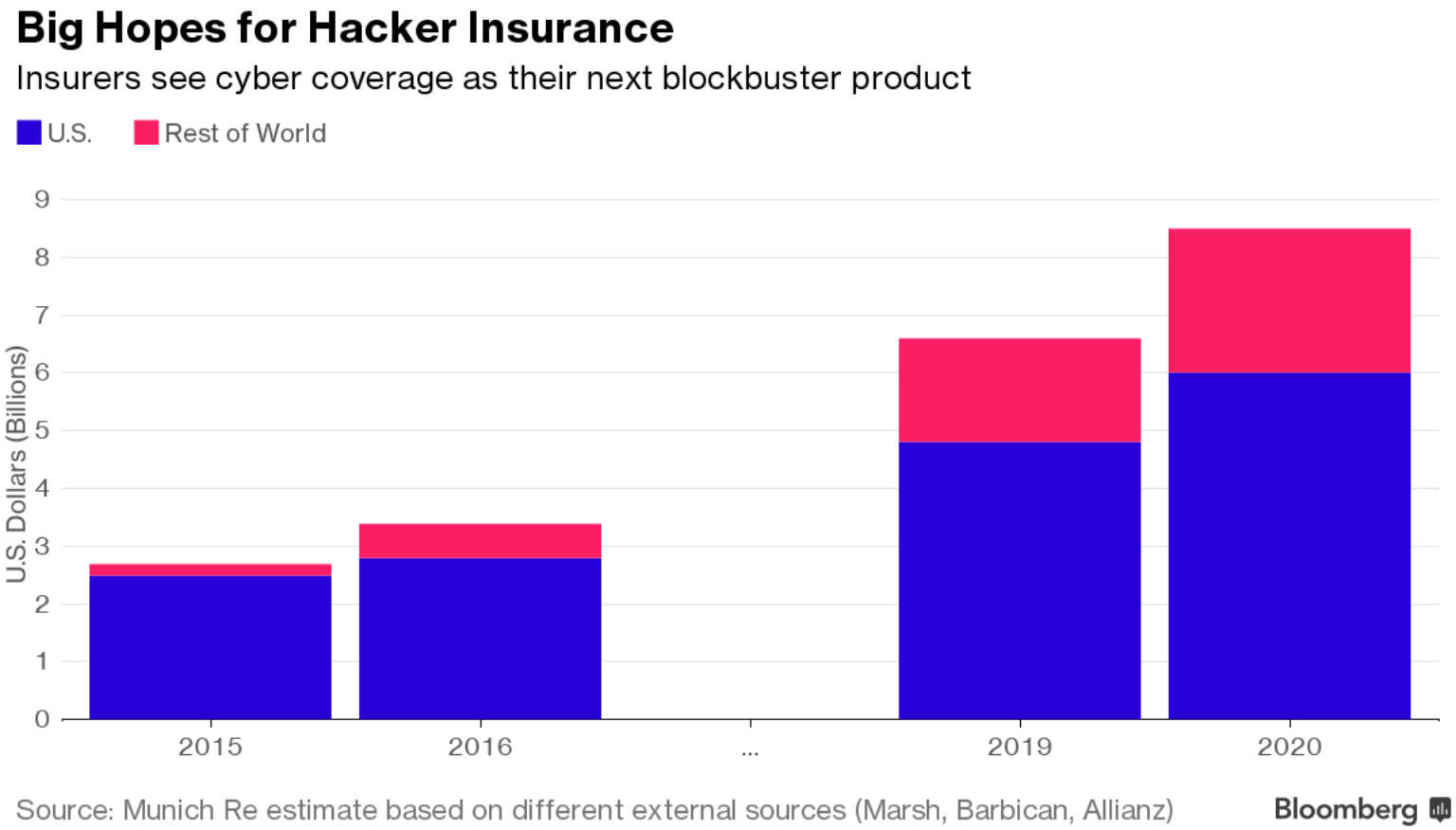
- Just about any organization that uses technology to do business faces cyber risk.
- And as technology becomes more complex and sophisticated, so do the threats we face – which is why every business and organization should be prepared or at least discuss cyber liability insurance and an effective cyber security plan to manage and mitigate cyber risk.

4 Ways Cyber Insurance Helps Protect a Business

- Lost Data – covers breach of data
- Lost Devices – prevents unauthorized use
- Notification Requirements - Notifying customers or clients of a breach and other post-breach responses, which is mandated by law, can be costly
- Forensics – Private client information compromised?

Ponemon Institute 2016 Cost of Data Breach Study

Insurers see Cyber Coverage as Blockbuster Product



What is Digital Evidence?

Digital evidence is any information or data of value to an investigation that is stored on, received by, or transmitted by an electronic device. Text messages, emails, pictures and videos, and internet searches are some of the most common types of digital evidence.

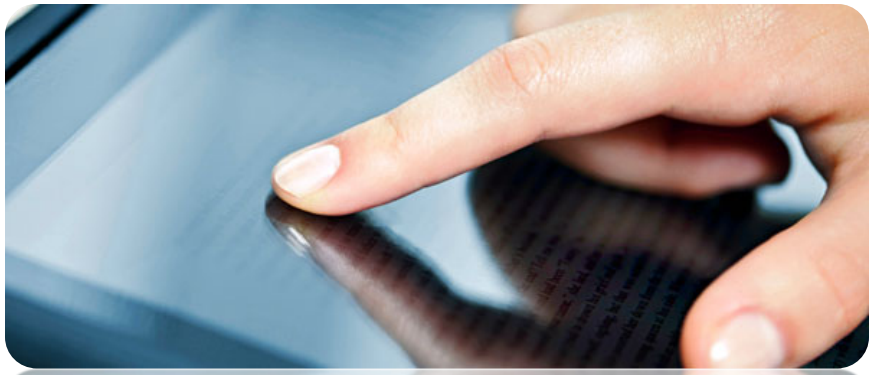
The Digital Trail

Most criminals now leave a digital footprint; a suspect's IP address, posting on a Social Media platform or using their mobile device for everyday use in place of a traditional computer and camera. This is information could reveal:

1) Intent,
2) Location and time of crime,
3) Relationship with victim(s), and
4) Relationship with other suspect(s)

More on Digital Evidence:

- It is latent (hidden), like fingerprints or DNA evidence;
- Crosses jurisdictional borders quickly and easily;
- Can be altered, damaged or destroyed with little effort; and
- Can be time sensitive.



How Digital Evidence and Intellectual Property Issues Intertwine:

What is Intellectual Property?

- Intellectual property (IP) refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce.
- IP is protected in law by patent, copyright and trademarks, which enable people to earn recognition or financial benefit from what they invent or create. By striking the right balance between the interests of innovators and the wider public interest, the IP system aims to foster an environment in which creativity and innovation can flourish.

What is Intellectual Property?

Some states, including Illinois, have their own trademark procedures for protecting names for goods or services used within the state. All these facets of the intellectual property law cooperate to provide the maximum protection for an idea, an invention, a work of art, a book or other item of intellectual property.

Digital Evidence in a IP Case

- Intellectual property litigation will rise and fall with the digital evidence. Consider the facts:
- Over 99 percent of corporate documents are created electronically.
- Fewer than one third of e-documents are ever printed.
- As many as 420 billion e-mails were sent each day in 2016.
- An estimated 60 percent of a business' critical e-mail information is contained within corporate e-mail systems.

Potential sources of evidence created outside of the day-to-day operations of corporations:

- Webmail providers;
- Internet service providers (ISPs);
- web-based or cloud application;
- Storage providers;
- Cellphone providers; and
- Government closed-circuit surveillance cameras;
- Highway toll systems


Imitation is the sincerest form of intellectual property theft.
yourecards
someecards.com

Seized Devices in an Investigation:

- Smartphones and other mobile devices;
- Laptops and Computer Desktops;
- CDs, DVDs, digital camera, surveillance systems, GPS devices, thumb drives

Data Breach Fact:

Yahoo

- Date: 2013-14
- Impact: 3 billion user accounts
  Details: In September 2016, the once dominant Internet giant, while in negotiations to sell itself to Verizon, announced it had been the victim of the biggest data breach in history, likely by “a state-sponsored actor,” in 2014. The attack compromised the real names, email addresses, dates of birth and telephone numbers of 500 million users. The company said the "vast majority" of the passwords involved had been hashed using the robust bcrypt algorithm.
- Besides names, dates of birth, email addresses and passwords that were not as well protected as those involved in 2014, security questions and answers were also compromised.
- In October of 2017, Yahoo revised that estimate, saying that all 3 billion user accounts had been compromised.