October 25, 2018
CIO Government Technology Conference
The Pyramid Club, Philadelphia

Minimizing Legal Risk from Cyber and Privacy Infractions

Luncheon Keynote Speech

Presented by **Gerry J. Elman, J.D.**

Welcome to The Pyramid Club in Philadelphia

Elman Technology Law, P.C.

STRATEGIC LAWYERING. CULTIVATING INNOVATION.®

Overview of cybersecurity landscape

- Old: fewer connected users and devices, anti-virus software would protect your PC. Businesses communicated with customers by letter, phone and fax.
- New: the world is connected. Businesses and individuals communicate using multiple digital platforms.
- Public perception: "But I'm not a target. (It's just the military / big business / movie stars / politicians … who have to worry)"
- Reality: Countless bad actors attack all systems to extract data they can use, or sell, or inactivate systems to gain an advantage. Nobody is immune.

Total Number of Breached Records*

(*that we know of)

- Records Breached: 11,237,709,895
- from 8,865 DATA BREACHES made public since 2005

Source: https://www.privacyrights.org/data-breaches (10/24/2018)

Equifax data breach

- A 2017 data breach exposed the sensitive personal information of 143 million Americans. A GAO report of 9/7/2018 confirms that a single Internet-facing web server with out-of-date software led to the breach, which went undetected for 76 days. Attackers made 9,000 queries that were unnoticed due to a failure to keep a network-data inspection system up to date. It hadn't worked for 10 months before staff noticed. Attackers accessed a database that contained unencrypted credentials that they used to access other internal databases.
- At the end of 2017, the cost from the data breach was **$439 million**. Of that, Reuters noted Equifax said **$125 million** will be covered by an insurance policy. Larry Ponemon, chairman of Ponemon Institute, told Reuters the final cost of the breach could end up being more than **$600 million**.
- https://www.ftc.gov/equifax-data-breach
- http://fortune.com/2018/09/07/equifax-data-breach-one-year-anniversary/

Facebook data breach

- 30 million Facebook users had their information exposed recently
- The hackers accessed only a limited subset of the data they could have taken, Facebook said last week. Instead of accessing personal messages, they accessed contact details—including phone numbers and email addresses—gender, relationship status, and search and check-in data belonging to 14 million users. For another 15 million users, only names and contacts were accessed; and the attackers didn't obtain personal information from 1 million people affected by the breach.
- Hackers gained access to the accounts by exploiting a vulnerability in Facebook's "view as" feature, which lets people see how their profiles appear to others. Three obscure bugs in Facebook's code allowed the outsiders to steal the data.
- https://www.wsj.com/articles/facebook-tentatively-concludes-recent-hack-was-perpetrated-by-spammers-1539821869

Healthcare.gov data breach

- Hackers breached a system connected to the healthcare.gov site, exposing the personal files of about 75,000 people, according to the Centers for Medicare and Medicaid Services (Oct. 22, 2018)

Small businesses are targets but many owners are willfully blind

Category	Fact
Small business level of readiness	78% of have no response plan in place
Small businesses already breached	54% admitted being victims of specific types of cyber attacks (virus, phishing, hacking, unauthorized access to company or customer data)
Most small business owners without a response plan don't think this affects them	45% said they don't think their company will be affected by a cyberattack

Source:
https://www.nationwide.com/about-us/101316-cybersecurity.jsp

A Better Aproach to Cybersecurity

not this…

Image: "I Can't See You" by Peter at https://flic.kr/p/5q67Vu.
Used under Creative Commons License CC BY-SA 2.0

Cybersecurity and Privacy Laws

U.S. Federal

- Financial institutions: Fair Credit Reporting Act, Gramm-Leach-Bliley Act, Red Flags Rule
- Health Insurance Portability and Accountability Act ("HIPAA")
- Health Information Technology for Economic and Clinical Health ("HITECH")
  - Strengthens cybersecurity provisions of HIPAA, requires breach notification, etc.
- Computer Fraud and Abuse Act ("CFAA")
- Cybersecurity Act of 2015
- Children's Online Privacy Protection Rule ("COPPA")
- FTC authority

Cybersecurity and Privacy Laws

- **State and Foreign**
  - European General Data Protection Regulation ("GDPR")
    - Went into effect with much fanfare May 25, 2018
    - Made by: European Parliament and Council of the European Union
    - Protects personal data of EU residents worldwide, with harsh penalties
  - New York State Cybersecurity Requirements for Financial Services (effective March 1, 2017)
  - California Consumer Privacy Act of 2018 ("CCPA")
    - Enacted June 28, 2018, to become effective Jan. 1, 2020
    - Beefs up California Online Privacy Protection Act ("CalOPPA")
    - Similar to GDPR, will be subject to amendment
  - Various state privacy breach notification laws
    - Have been in effect for a few years, patchwork quilt

Identity Theft Regulations

- Primary federal ID theft regulations stem from the Fair and Accurate Credit Transactions Act of 2003.
- FTC, OCC, FDIC, SEC, and CFTC are charged with enforcement of law.
- “Financial institutions” and some “creditors” required to implement written ID theft prevention designed to catch, stop, and prevent ID theft and its costly consequences.

How does a cyber-security claim arise?

- There is valuable information in a system the operator hopes is secure.
- But a bad actor gains access through a technical vulnerability or by trickery and can then:
  - Breach the system, secretly copy the information and sell information including:
    - Personally Identifiable Information (PII) about your customers, employees, and others
      - Useful for further identity theft efforts
    - Protected Health Information (PHI)
    - Trade secrets (corporate espionage)
  - Breach the system, secretly copy the information and publicize it
    - Hacktivism
  - Take control of an information system by ransomware, demanding payment to restore access to the information
  - Impersonate a business or agency, seeking to divert legitimate transactions (corporate identity theft)

How does a cyber-security claim arise?

- Customers, fearing identity theft, sue after a breach during which their PII was exfiltrated.
  - They allege the operator was negligent in failing to prevent the breach.
  - They allege it took too long before they were notified.
- Shareholders bring a derivative suit after an incident, accusing management of insufficient attention to cyber-security.
- Company/agency sues its information technology company for failing to provide the expected level of security.
- And/or sues cyber-breach remediator for failing to close a backdoor.
- Insurance company denies coverage for a cyber-incident and company/agency disputes it.
- Company gets sued by a regulatory agency for noncompliance with pertinent regulations
- Company gets sued for product liability when customer alleges an Internet-enabled gizmo has lax security.

How does a cyber-security claim arise?

- Or a bad actor launches a Denial of Service (DoS) attack against a system, e.g. by flooding the network with excessive requests that disrupt normal operation, or by altering or destroying network connectivity, data, or physical components.
- It is unusual to be able to identify the perpetrator of a cyber-breach or attack.

Liability for breached records

PA Breach of Personal Information Notification Act (PABPINA)

73 Pa. Stat. Ann. §2301 et seq.

Businesses must notify PA residents if residents' personal information was in a breached database.

- Breach
  - "The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth." (excludes good faith acquisition by agent of entity)

PA Breach of Personal Information Notification Act (cont'd)

- Personal Information
  - First name or first initial and last name combined with unencrypted/unredacted data including:
    - Social Security number.
    - Driver's license number or equivalent state ID card number
    - Financial account number, credit or debit card number, in combination with code or password enabling access to the account
- Records
  - Any information except information that the individual has voluntarily made public (i.e, name, address, telephone number).
- Notification Requirement
  - to all Commonwealth residents whose records were breached, "without unreasonable delay"
  - Exception: if the breached entity follows its own breach incident response notification policy

PA Breach of Personal Information Notification Act (cont'd)

- Consumer credit agencies:
  - If over 1,000 records are breached at once, the entity also has to notify the credit bureaus.
- Encryption is not a perfect shield:
  - Notice required if encrypted data is obtained in unencrypted form, if breach is linked to security of the encryption or if breach involves a person with access to the encryption key
- Violations
  - A violation "shall be deemed to be an unfair or deceptive act or practice". The Attorney General can bring an action under the UTPCPL.
- Notice methods
  - written, phone, e-mail, and can include substitute methods if the cost of notice otherwise is over $100,000

The takeaway from the PABPINA:

- Encrypt Personal Information
- Redact Social Security Numbers
  - Bonus: this also protects you from violating the PA Social Security Number Privacy Act (74 Pa. Stat. Ann. § 201)
- Don't store unnecessary Personal Information
- Avoid a breach!

PCI Compliance

Do you accept credit cards? …Of course you do!

- PCI Compliance: If your company accepts credit card payment, you have to certify that you follow certain safeguards to protect the cardholder's information.
- The latest standard is PCI-DSS 3.2.1, released May 2018.
- Your credit card processor requires that you comply with annual certification.
- Credit card companies (Visa, MasterCard, etc.) require that member banks ensure security, and banks require that merchants ensure security.

The PCI Data Security Standard

PCI DSS has over 250 sub-requirements, but these are essentially:

Six Goals, 12 Requirements

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1: Install and maintain a firewall configuration to protect cardholder data 2: Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3: Protect stored cardholder data 4: Encrypt transmissions of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5: Use and regularly update anti-virus software 6: Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7: Restrict access to cardholder data by business need-to-know 8: Assign a unique ID to each person with computer access 9: Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10: Track and monitor all access to network resources and cardholder data 11: Regularly test security systems and processes
Maintain an Information Security Policy	12: Maintain a policy that addresses information security

Source: https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/site-data-protection-PCI.html

If Your Customers' Credit Card Information Is Lost or Stolen…

- Fines and Penalities
  - For Non-compliance with PCI-DSS (remember, you certified that you were compliant!)
- Repayment of costs to credit card company
  - for investigation, remediation, etc.
- Repayment of costs to issuing bank
  - which was fined by credit card company because you weren't compliant
- Legal compliance issues
- Very unhappy customers

Develop a Computer Security Incident Response Plan (CSIRP)

- Policy prepared before a crisis and kept up to date
- Identifies the team, and who will be responsible for what actions
- How to respond in immediate aftermath
  - Stop ongoing breach
  - Preserve forensic data
  - Notification
  - Comply with law
  - Public relations
- FOLLOW THE PLAN.

Benefits of a CSIRP

- If you've taken steps to prepare for a breach, and you have a procedure for responding to a breach, you benefit:
  - Lower costs
  - Lower likelihood of successful litigation
  - Higher level of client/customer trust
  - Easier to operate; lower level of crisis
  - Better public relations
  - More likely that you'll survive and thrive

Get a Cybersecurity Legal Audit

Because you don't know what you don't know.

"As we know, 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."

-Donald Rumsfeld, Secretary of Defense to President George W. Bush

How to Protect Your Company and Your Customers

- Cybersecurity Legal Audit
  - Have a cybersecurity lawyer review your legal posture
  - Network penetration testing performed by vendor at direction of lawyer (protected by attorney-client privilege)
  - Develop breach incident response system
  - Review of risk mitigation options, including cyber insurance
- Update internal policies
- Update website / app policies
- Limit storage of personal information, and secure what you have

Gain the Protection of Attorney-Client Privilege

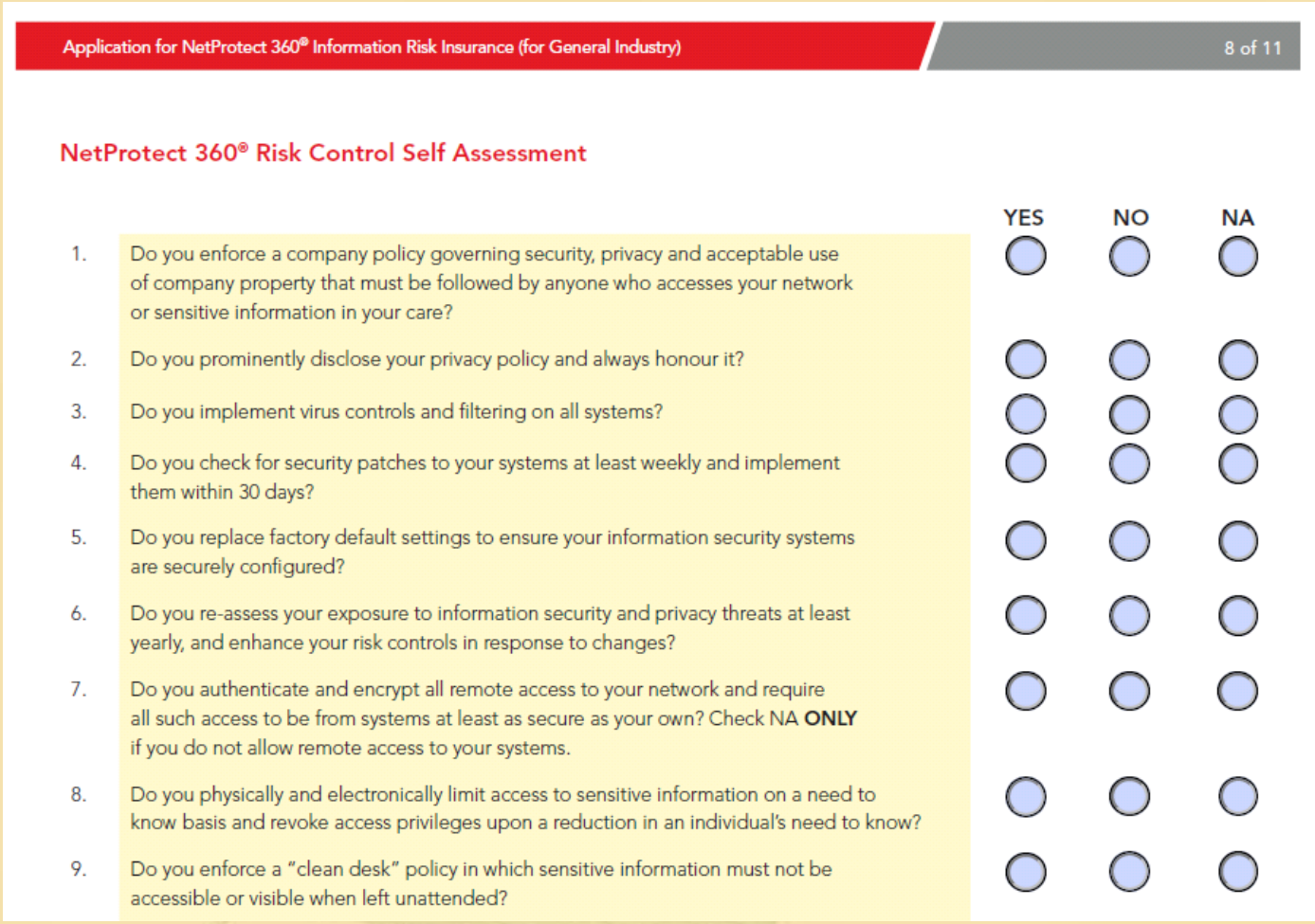
- *Genesco, Inc. v. Visa, Inc.*, No. 3:13-cv-00202 (M.D. Tenn.) Order entered on March 25, 2015
- Extensive litigation over multi-million dollar fines by Visa against Genesco for data breach

"[t]o be sure, the information sought in [Visa's] motion to compel is relevant and probative[,] . . . Plaintiff retained IBM to provide consulting and technical services so as to assist counsel in rendering legal advice to Plaintiff. Thus, the IBM materials . . . [were] privileged."

- **Summary: Hire a lawyer to evaluate and improve your legal and tech cybersecurity compliance, with the technology firm working at the direction of the lawyer.**

See Austin Morris or Michael Fields for Cyber Insurance

- Review cyber insurance options with an experienced broker and your attorney.
- Know how you specifically handle data; don't assume.



Application for NetProtect 360® Information Risk Insurance (for General Industry) 8 of 11

NetProtect 360® Risk Control Self Assessment

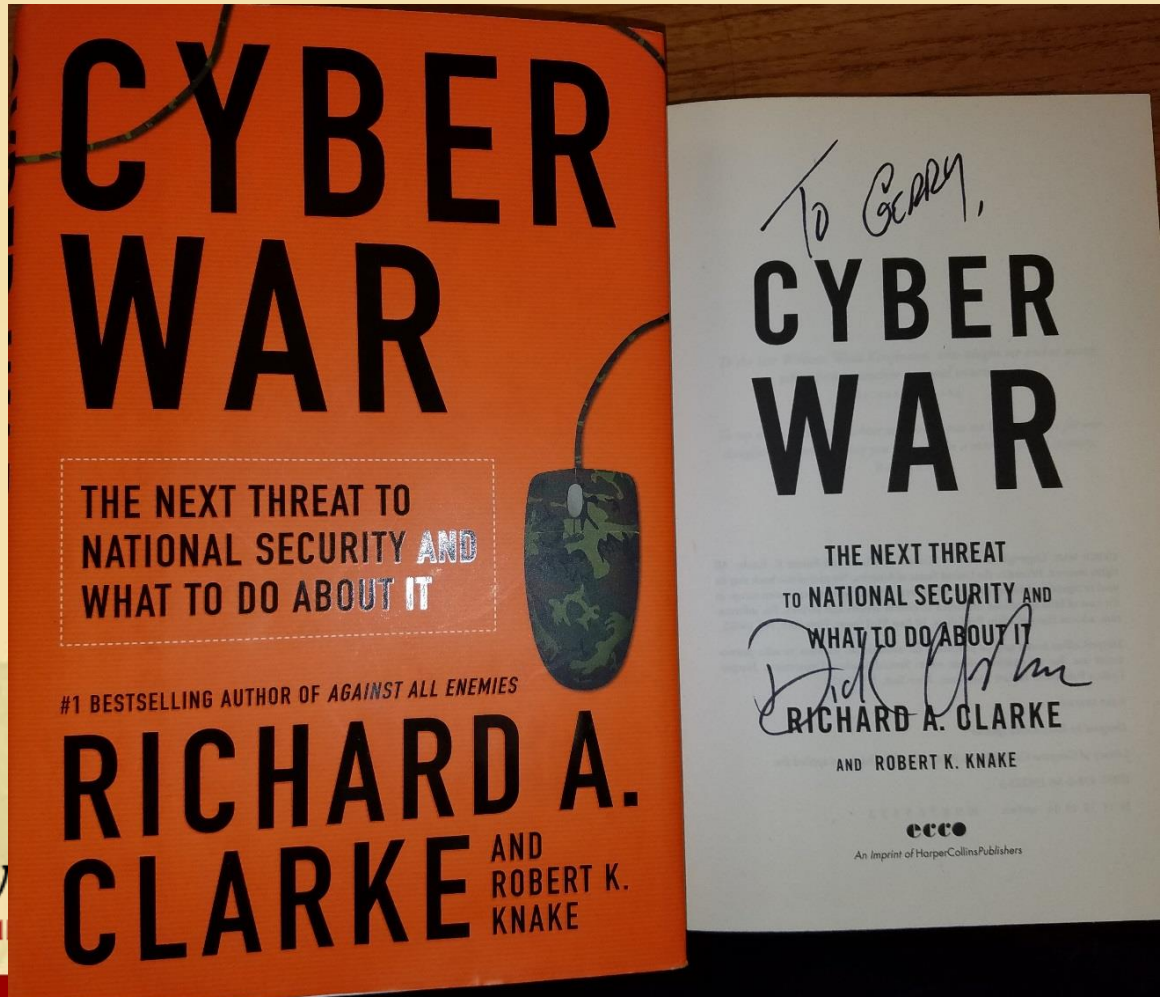
		YES	NO	NA
1.	Do you enforce a company policy governing security, privacy and acceptable use of company property that must be followed by anyone who accesses your network or sensitive information in your care?	○	○	○
2.	Do you prominently disclose your privacy policy and always honour it?	○	○	○
3.	Do you implement virus controls and filtering on all systems?	○	○	○
4.	Do you check for security patches to your systems at least weekly and implement them within 30 days?	○	○	○
5.	Do you replace factory default settings to ensure your information security systems are securely configured?	○	○	○
6.	Do you re-assess your exposure to information security and privacy threats at least yearly, and enhance your risk controls in response to changes?	○	○	○
7.	Do you authenticate and encrypt all remote access to your network and require all such access to be from systems at least as secure as your own? Check NA **ONLY** if you do not allow remote access to your systems.	○	○	○
8.	Do you physically and electronically limit access to sensitive information on a need to know basis and revoke access privileges upon a reduction in an individual's need to know?	○	○	○
9.	Do you enforce a "clean desk" policy in which sensitive information must not be accessible or visible when left unattended?	○	○	○

$16 million fine by HHS OCR

- Anthem – 79 million patients' data exposed
- The Office of Civil Rights at the Dept. of Health and Human Services announced last week that health insurer Anthem Inc. had agreed to a record $16 million HIPAA settlement in the wake of a cyberattack revealed in 2015, which impacted nearly 79 million individuals. In announcing the largest-ever HIPAA fine, regulators noted the insurer failed to take several basic security steps, including conducting an enterprisewide security risk assessment.
- However, Anthem had announced in September 2013 that it had been certified as compliant with the HITRUST Common Security Framework. Federal regulators said the cyberattackers likely began their intrusions in February 2014, about five months after the insurer achieved HITRUST certification.

Cyber War is Here

- More than just compliance with laws; be strategic in your thinking and practices



For Further Information…

Elman Technology Law
(610) 892-9942

www.elman.com
gerry@elman.com

12 Veterans Square, Media, PA

About Gerry Elman

Gerry Elman is the president of Elman Technology Law, P.C. in Media, Pennsylvania. He generally advises on intellectual property and Internet business law, and helps clients minimize the financial and reputational risk that can result from a variety of cybersecurity breaches.

He's a seasoned patent attorney and has also served in Harrisburg as a state Deputy Attorney General and as trial attorney with the federal Antitrust Division. He has science degrees from Stanford and the University of Chicago, and earned his law degree at Columbia. He is also a widely published author on technology and the law and has been working with computers and online information since the early 1980s.

About Elman Technology Law

Elman Technology Law, P.C. lawyers advise clients on intellectual property and Internet-related business matters, helping them develop strategies to maximize their ability to leverage intellectual assets and protect the "crown jewels" of their businesses. With regard to cybersecurity, we help clients comply with state and federal laws and standards, to minimize risk of adverse results in litigation over the inevitable breach of cybersecurity.

As a boutique law practice in a suburb of Philadelphia, we can advise law firms on the ethical, legal and technical requirements for protecting confidential client information. With our guidance, they can thus reduce financial and professional exposure regarding loss of such information.