ALFA International
The Global Legal Network
Local Relationships Worldwide

ALFA International
The Global Legal Network

ALFA International
The Global Legal Network
Local Relationships Worldwide

ALFA International Regional Seminar on Product Liability Legal Issues

April 11, 2019
Charlotte, North Carolina

Product Hacking, Cyber Security for Products, and the Internet of Things

ALFA International
The Global Legal Network
Local Relationships Worldwide

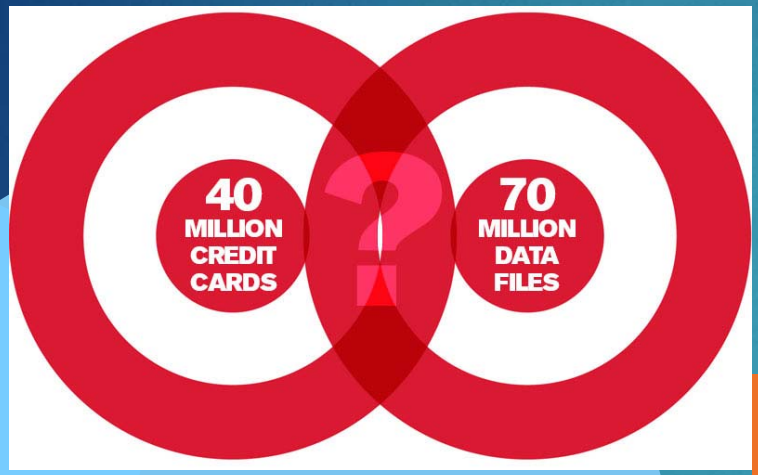
Presenters

S. Christopher Collier
Atlanta, Georgia

HAWKINS PARNELL
Hawkins Parnell & Young, LLP

ALFA International
The Global Legal Network
Local Relationships Worldwide

Data Breach: The New Frontier of Corporate Catastrophes



ALFA International
The Global Legal Network
Local Relationships Worldwide

What is Information Security?

ALFA International
The Global Legal Network
Local Relationships Worldwide

What is Information Security?

Protects following characteristics:

- **Confidentiality** - Who can see the data?
- **Integrity** – Who can change the data?
- **Availability** – Ensuring that the data is available to authorized people.

- "IT security in 2019 is no longer going to simply be about protecting sensitive data and keeping hackers out of our systems. In this day and age of ***big data and artificial intelligence—where cooperation on data can lead to enormous business opportunities and scientific and medical breakthroughs***—security is also going have to focus on enabling organizations to leverage, collaborate on and monetize their data without being exposed to privacy breaches, giving up their intellectual property or having their data misused."

Rina Shainski, Co-founder and Chairwoman, Duality Technologies

Cybersecurity Predictions for 2019, Forbes

New Cyber Risks

- Duty to create products better than human
- Duty to recognize and intervene when software is malfunctioning
- Standard higher than reasonable person

What Must Be Protected?

- User information
- Location
- Preferences
- Financial information

ALFA International
The Global Legal Network
Local Relationships Worldwide

Common Cyber Threats

- Email Account Takeover
- Malware
- Phishing
- Credential Replay
- Social Engineering
- Call Forwarding
- Spoofing

Sources of Threats

Internal Threats

- Disgruntled Employees
- External Contractors
- Employees that are negligent, misinformed, or have made a mistake

External Threats

- Hackers
- Foreign Countries
- Corporate Spies
- Protesters
- Organized Crime

Which industries are most susceptible to data breach?

ALFA International
The Global Legal Network
Local Relationships Worldwide

Nobody is exempt...

- Blur (password manager service)
- 500px (photo sharing website)
- Huddle House
- Fortnite (popular online video game)
- UConn Health

ALFA International
The Global Legal Network
Local Relationships Worldwide

Tactics, techniques, and procedures

- Spear-phishing emails (from compromised legitimate account)
- Watering-hole domains
- Credential gathering
- Open-source and network reconnaissance
- Host-based exploitation
- Targeting industrial control system (ICS) infrastructure
- Ransomware
- Company website or VPN

Product Hacking, Cyber Security for Products, and the Internet of Things

Consequences of Security Breaches

Consequences of Security Breaches

Consequences

- **Confidentiality** - Risk to personal or confidential information.
- **Integrity** - Data corruption or destruction.
- **Availability** - Unavailability of business data or critical information in an emergency, etc. (Email, ERP, etc.)

Other Consequences:

- Loss of trust from employees and the public.
- Impact on Brand.
- Costly reporting to the government and remediation requirements.
- Potential for large fines, penalties and lawsuits.

ALFA International
The Global Legal Network
Local Relationships Worldwide

Product Hacking, Cyber Security for Products, and the Internet of Things

Consequences of Security Breaches

Legal Considerations: Reporting

ALFA International
The Global Legal Network
Local Relationships Worldwide

Data Security and Breach Notification Act

Proposed Federal Law would:

- Require companies to notify consumers that they have had a breach within 30 days.
- Institute a maximum five-year prison sentence for intentionally hiding such a breach.
- Create financial incentives for companies or organizations that utilize technologies which make consumer information unreadable in the event of a breach.

Senate Bill 2179, Nov. 2017

State Security Breach and Notification Laws

"All 50 states, DC, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches of personally identifiable information."

http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

ALFA International
The Global Legal Network
Local Relationships Worldwide

Cyber Security Plans Should be Tailored to State Law Requirements

- Who must comply?
- What constitutes a breach?
- Who must be notified?
- Any exemptions?

ALFA International
The Global Legal Network
Local Relationships Worldwide

States That Permit a Private Cause of Action

- Alaska, California, Illinois, Louisiana, Maryland, Massachusetts, Nevada, New Hampshire, North Carolina, Oregon, South Carolina, Tennessee, Texas, Virginia, Washington, District of Columbia, Puerto Rico, and Virgin Islands.

Product Hacking, Cyber Security for Products, and the Internet of Things

Key Current Security Risks & Mitigation Approaches

ALFA International
The Global Legal Network
Local Relationships Worldwide

Cyber Defenses

- Two-factor authentication
- Employee education
- Vetting of vendors/contractors
- Maintaining software updates

ALFA International
The Global Legal Network
Local Relationships Worldwide

Mitigation

- Include analog controls
- Insurance
- Cyber security plan
- Contractual provisions
- Regulations

United States Computer Emergency Readiness Team

- Maintain up-to-date antivirus protection
- Restrict permissions to install and run unwanted software applications
- Enforce a strong password policy and regular password changes
- Exercise caution when opening e-mail attachments
- Keep operating system patches up-to-date
- Scan and remove suspicious e-mail attachments
- Monitor users' web browsing habits; restrict access to sites
- Exercise caution when using USB drives, external drives, etc.
- Scan all software downloaded from the Internet prior to executing
- Maintain situational awareness of the latest threats

Data Breach

Model Security Breach Response

- **Model security breach response plans**
  - intended to complement a company's data security program
  - designed to ensure that appropriate protections are in place.
- These are used to determine which individuals must be notified following a data breach.
- Counsel must review and stay up to date on both state and federal laws governing data breaches in your industry to update the plans.

Data Breach

Model Security Breach Response Plans:

Role of In-House Counsel in preventing data breach

As counsel for these companies, our role is to manage, oversee, and coordinate remediation following an incident

ALFA International
The Global Legal Network
Local Relationships Worldwide

Data Breach

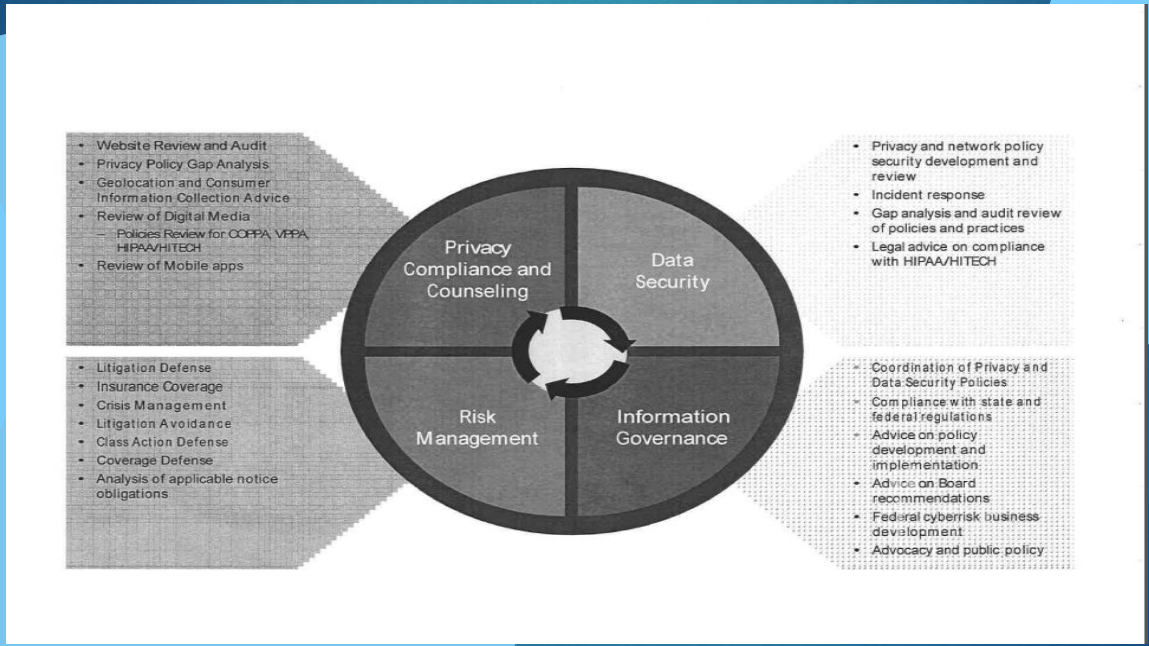
Statutory Data Breach Notification Requirements:

- Identify the states and countries potentially involved in the breach by determining location of the customers, employees, and systems affected by the breach.
- Identify federal, state, and international statutes and regulations potentially triggered or violated by the breach.

ALFA International
The Global Legal Network
Local Relationships Worldwide

Data Breach

Model Security Breach Response Plans:



ALFA International
The Global Legal Network
Local Relationships Worldwide

Product Hacking, Cyber Security for Products, and the Internet of Things

Questions

ALFA International
The Global Legal Network
Local Relationships Worldwide