Protecting Facilities and Balance Sheets: The SAFETY Act

Brian E. Finch

DICKSTEINSHAPIROLLP

AGA American Gas Association

EEI Edison Electric Institute

An Overview of Where We Stand

Pre and Post 9/11liability concerns

- Pre/911, claims following terrorist attacks were dismissed (related to 1993 and 1995 attacks):
  - Courts found that no jury could reasonably conclude that terrorist attacks were anything more than a remote or theoretical possibility, and that the terrorists precluded arguments that the plaintiffs might have had against the defendants.
- Post 9/11, claims have been allowed to move forward:
  - Courts found that the terrorists actions on 9/11 were reasonably foreseeable, and a duty was owed to the plaintiffs.
  - The danger of a plane crashing as a result of a hijacking was "the very risk that Boeing should reasonably have foreseen."
  - Courts also have found that if a defendant "knew or should have known" of a threat, they have to take "reasonable" mitigation steps.
  - Defined as steps could be ones that previously were considered "burdensome," or even the most stringent of mitigation measures suggested in the course of a vulnerability assessment.

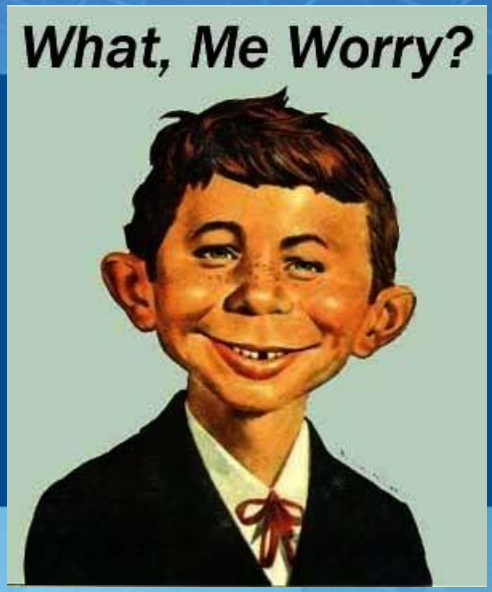
Why Will Plaintiffs Sue Security Providers Or Infrastructure Owners?

- Recover From Terrorists?
  - The widow of murdered journalist Daniel Pearl has withdrawn a lawsuit seeking damages against al-Qaida, a dozen reputed terrorists and Pakistan's largest bank. [L]awyers noted that the defendants in the case had not answered the lawsuit filed in July.
- Recover From State Sponsors?
  - Beirut Bombing: A Federal judge ordered Iran to pay $2.65 billion to relatives of the 241 American military people killed in a 1983 bombing in Lebanon and to 26 survivors of the attack, a ruling that is likely to remain symbolic. How the nearly 1,000 plaintiffs can recover the damages is unclear, since Iran is estranged from the U.S., has denied responsibility for the attack, *and did not even respond to the lawsuit.*
- That leaves security providers and property owners as the deep pockets.

Remember … Litigation WILL HAPPEN

- Families who sued after 9/11 were not motivated by money
- Litigants said the 9/11 Compensation Fund was "hush money"
  - "People were being paid off not to go to court"
- Litigation was viewed as a way to get accountability
  - "What I'm looking for is justice … someone held accountable … there are people who did not do their job"
- If they could do it again, more people would sue
  - "I felt 'dirty' after taking the money"
- The legal bills? Hundreds of millions of dollars …
- Settlement fund participants received $2m/average vs. $5m/average for people who brought lawsuits

The Cyber Threat



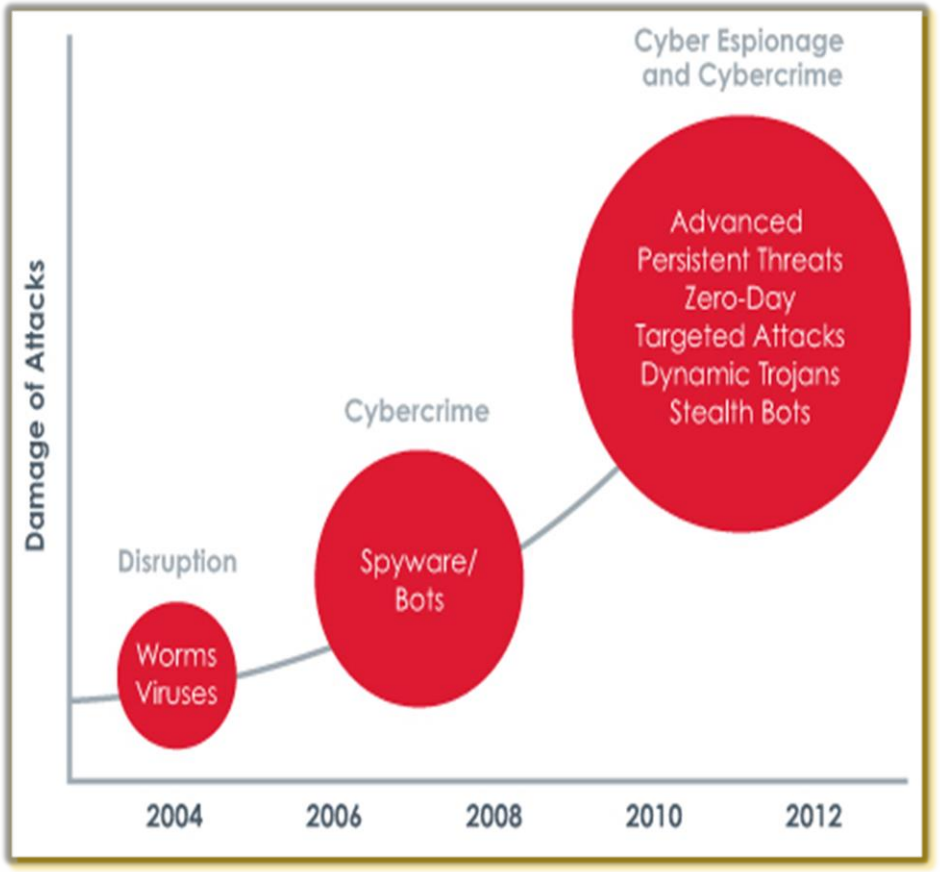
The Good Ole Days of Espionage

Cyber Data Breaches

- Not if, not when, **but how often**
- Disruption/Destruction of Operations
- Destruction of data
- Exposure of corporate secrets, trade secrets, and other proprietary information
- Attacks are **CHEAP**:
  - $2/hour for denial of service attack
  - $30 to check against standard anti-virus programs
  - $5000 for a totally new, “zero day” attack program

Advanced Persistent Threats

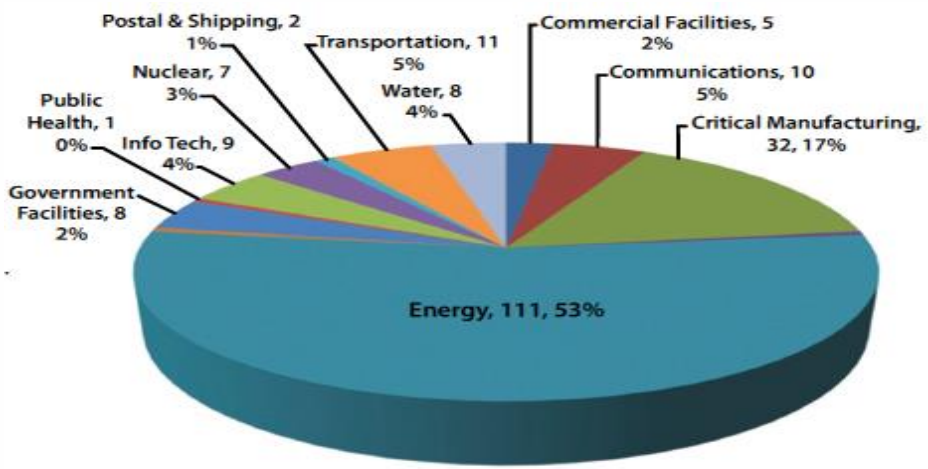
- Bypassing traditional security and sitting undetected on systems
- Difficult to detect and defeat due to the advanced resources put into development and deployment
- Most worrisome are “signature-less” threats … criminals with no fingerprints
- When APT detection systems are installed, approximately **20-fold** increase in discovery of attacks
- Anti-virus is “yesterday’s news”



Source: http://www.fireeye.com/threat-protection/

SCADA Attacks On The Rise?

- Reported SCADA attacks were up 100% from 2012, according to ICS-CERT:



- Severity and actual impact? Unknown. EXCEPT people are reacting (DOD imposing cybersecurity requirements on SCADA systems).

The “C-Suite” Cares – A Lot

Data Security is #1 Concern of Directors & General Counsel

Legal Risks On the Radar

Figure 1
Top 10 concerns for directors and general counsel:

Directors	
Data security	48%
Operational risk	40%
Company reputation	40%
M&A transactions	37%
Investor relations	36%
Executive compensation	36%
SEC/regulatory compliance	28%
Disaster recovery	27%
Internal controls	26%
Global business expansion	26%
General Counsel	
Data security	55%
Operational risk	47%
Management of outside legal fees	38%
Company reputation	35%
Disaster recovery	35%
E-discovery	33%
FCPA	30%
Global business expansion	29%
Internal controls	26%
Executive compensation	26%

Figure 2
Directors who say their company has a crisis management plan in place to respond to a cyber attack.

Introduction
Each year, Corporate Board Member and FTI Consulting, Inc. conduct research to gain insight on which current legal issues raise concern for public company directors and corporate general counsel and to analyze related legal and governance events and trends. In early 2012, the organizations gathered data by surveying 11,340 directors and 1,357 general counsel. Questions were asked of both groups to compare and contrast their perspectives; other queries were specifically targeted toward either directors or GCs. The 2012 Law and the Boardroom survey results that follow once again offer interesting insight into the thoughts and opinions of these two critical governance groups.

Executive overview
Several key themes emerged from the 2012 Law and the Boardroom study that reflect changes taking place within corporate America. During the past decade, for example, U.S. businesses have expanded globally and stepped up the use of online communication as well as web-based products and delivery channels. Thus, increasingly, corporate America is operating in a world where connectivity is high and there are few physical barriers. Accordingly, for the first time, data security was earmarked by the largest percentage of responding directors (48%) and general counsel (55%) as an issue of concern. The second most prevalent response for both directors and GCs centers on operational risk, which topped directors' list in 2011 and moved up several places for general counsel this year. Finally, on the risk/concern spectrum, directors and GCs flagged loss of reputation as an issue of critical concern in 2012.

A significant number of directors are also worried about risks related to mergers and acquisitions and their relationship with investors, while a significant number of general counsel noted concern with the management of outside legal fees and disaster recovery. Also resonating this year are issues involving compliance and investigations (Figure 1).

In addition to this barometer, the 2012 Law and the Boardroom study delved into opinions relative to proxy access and other shareholder-related matters. In particular, the study homed in on respondents' opinions regarding the nomination of director slates and subsequent actions taken as a result of 2011 say-on-pay votes. Also, for the first time, the survey queried respondents about the use of corporate social media and the risks and policies surrounding it. And finally, because the board/management relationship is a critical factor in the performance of the company, we asked directors and GCs to rate each other in several key aspects of effectiveness, as well as how well they work in tandem with each other.

The following report, a supplement to *Corporate Board Member* magazine's third quarter 2012 issue, presents highlighted data and examines each of these topics in fuller detail.

Cyber strategy and IT risk
Today, there is arguably no more insidious threat to a public company than that of cyber risk; it's invisible, ever-changing, and pervasive—making it very difficult for boards to manage. On top of that, it's costly. *Corporate Board Member* magazine recently reported that the median annualized cost of cyber crime per company averaged $5.9 million—a serious bottom-line expense. Thus, it comes as no surprise that this year, more than half (55%) of general counsel rated data security as a major concern and 48% of directors feel likewise. Interestingly, this level of concern has nearly doubled in the last four years: In 2008, only 25% of directors and 23% of GCs noted data security as an area of high concern.

2 Legal Risks on the Radar: The Corporate Board Member/FTI Consulting, Inc., 2012 Law and the Boardroom Study

CORPORATE BOARD MEMBER.
An NYSE Euronext Company

2012 SPECIAL SUPPLEMENT

DICKSTEINSHAPIROLLP

Possible Cyber Liability Claims

- Failure to:
  - remedy “known security vulnerabilities” such as allowing insecure server/network connections;
  - employ commonly used methods to require user IDs and passwords that are difficult for hackers to guess;
  - adequately inventory computers in order to manage network devices;
  - employ reasonable measures to detect and prevent unauthorized access or to conduct security investigations;
  - follow proper incident response procedures, including failing to monitor computer network for malware used in a previous intrusion; and
  - adequately restrict 3d party vendor access.
- 9/11 type claims?
  - Negligence/Negligent selection/Negligent design and/or manufacture, *Res Ipsa Loquitor, or even* Strict liability?

Is This Reasonable?

What About Newer Defenses?


REMAIN CALM!
ALL IS WELL!!!

The SAFETY Act

- "Support Anti-Terrorism By Fostering Effective Technologies Act".
- **Eliminates or minimizes liability** for sellers of DHS-approved cyber security technologies should suits arise after an attack (physical or cyber), including:
  - SAFETY Act protections can be obtained only by submitting an application to DHS.
  - Protections apply even if approved technologies are sold to **commercial** customers or if the cyber attack occurs **abroad**.

“Act Of Terrorism”

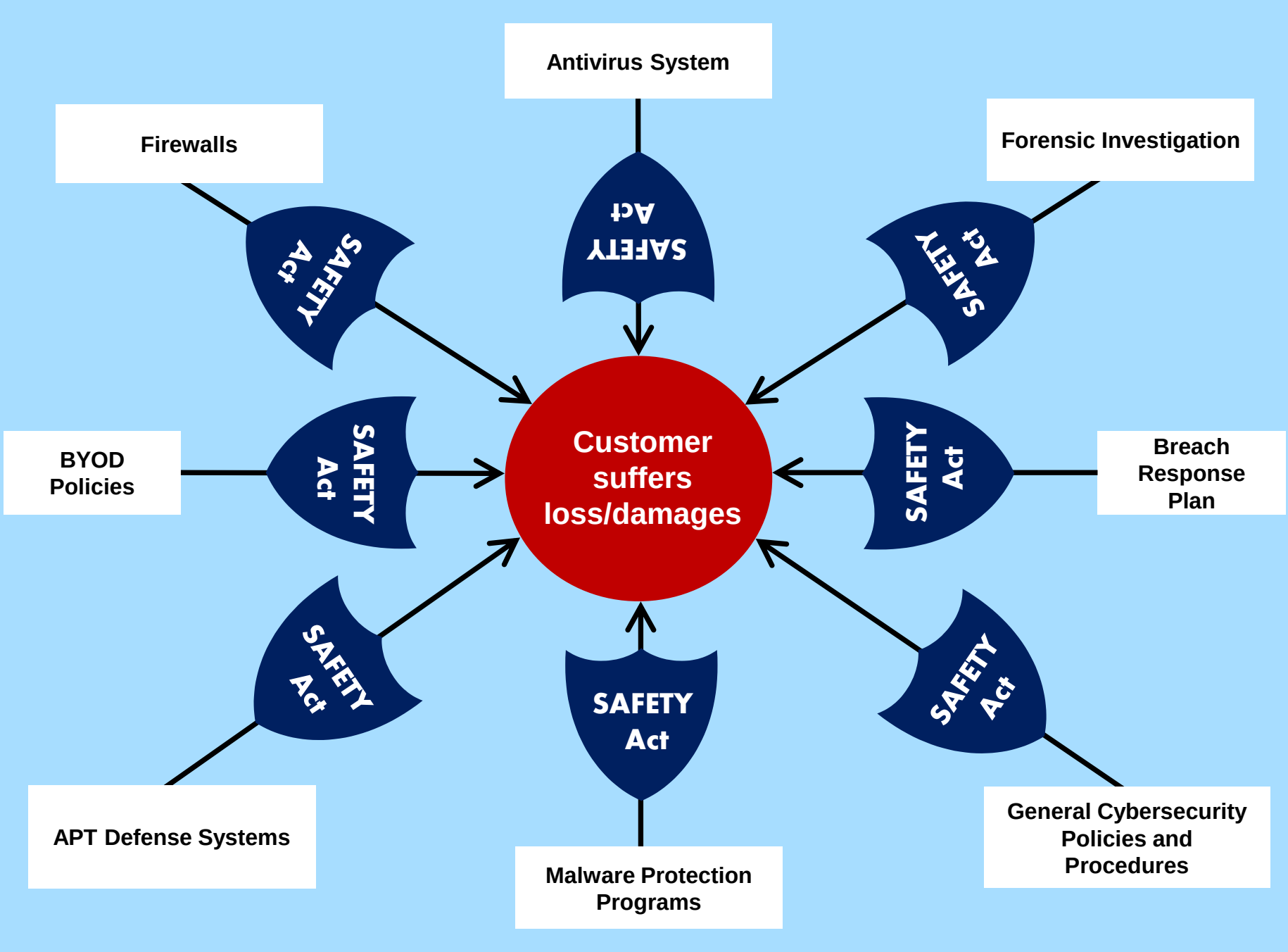
- What is an “act of terrorism”?
  - (i) is unlawful;
  - (ii) causes harm, including financial harm, to a person, property, or entity, in the United States, or in the case of a domestic United States air carrier or a United States-flag vessel in or outside the United States; and
  - (iii) uses or attempts to use instrumentalities, weapons or other methods designed or intended to cause mass destruction, injury or other loss to citizens or institutions of the United States.
- Definition is read to include events that impact the United States

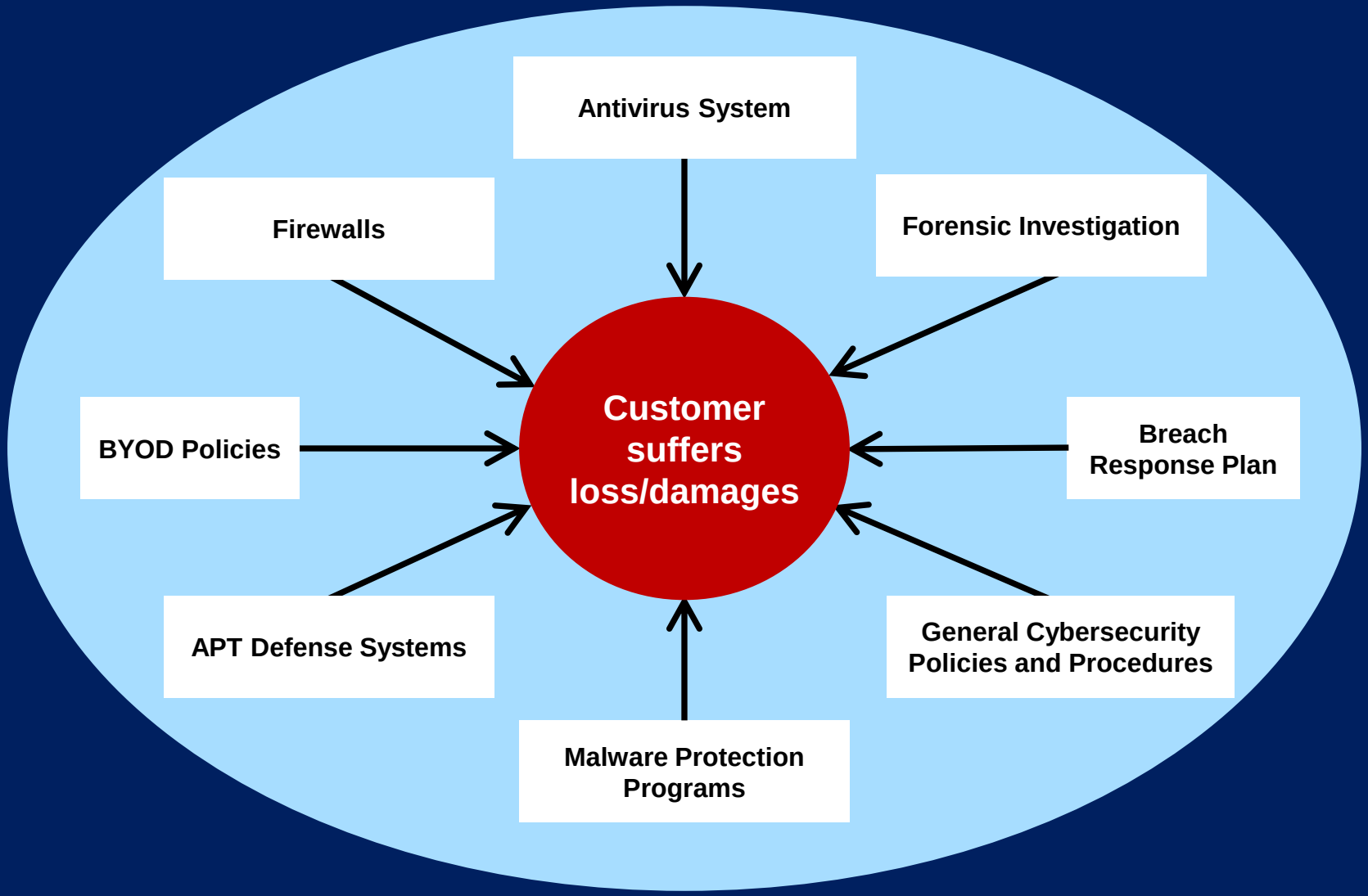
SAFETY Act: Designation Vs. Certification

- Two levels of protection under the SAFETY Act, Designation and Certification
- Under "Designation":
  - Claims may only be filed in Federal court
  - Damages are capped at a level set by DHS
  - Bar on punitive damages and prejudgment interest
- Certification offers all the same defenses PLUS presumption of immediate dismissal
- In both circumstances claims against **CUSTOMERS are to be immediately dismissed**

Cyber Attacks Trigger SAFETY Act Protections

- Any cyber security product, service, and/or policy is eligible for SAFETY Act protections.
- Cyber attacks are encompassed under this definition.
- There is NO requirement that the attacker's identity or motivation be identified/proven:
  - Only mention of "intent" potentially relates to intent to cause injury or loss, NOT traditional "terrorist" intent.
- This means that ANY cyber attack could potentially trigger SAFETY Act liability protections.


Antivirus System
Firewalls
Forensic Investigation
SAFETY Act
SAFETY Act
SAFETY Act
SAFETY Act
SAFETY Act
SAFETY Act
SAFETY Act
SAFETY Act
BYOD Policies
Customer suffers loss/damages
Breach Response Plan
APT Defense Systems
Malware Protection Programs
General Cybersecurity Policies and Procedures



Key Questions And How To Use

- Any costs for filing a SAFETY Act application? NO
- What kind of security products could be covered?
  - All *PRODUCTS, SERVICES, AND/OR POLICIES* are eligible for SAFETY Act protections.
- Could I get SAFETY Act protections for internal cyber or physical security plans? YES
- Can I get SAFETY Act protections for my NERC CIP Compliance Program? YES!!!
- What is the practical effect of obtaining SAFETY Act protections?
  - You could receive ***a cap on damages or immunity*** from damages arising out of or related to attacks.
- Can I realize SAFETY Act benefits just by purchasing and using SAFETY Act approved security solutions? YES
- Can I require SAFETY Act approval in procurements? YES

To Do List

- ✓ Review all current and planned physical and cybersecurity technologies, policies, and procedures to see which ones could be eligible for SAFETY Act protections.
- ✓ Start requiring all security vendors (physical and cyber) to apply for SAFETY Act protections.
- ✓ Line up SAFETY Act approved technologies with your insurance and compliance programs.

Questions/Comments/Thoughts?

Brian E. Finch
Partner
Dickstein Shapiro LLP
(202) 420-4823
finchb@dicksteinshapiro.com
Twitter: @BrianEFinch