GTSC

DICKSTEINSHAPIRO LLP

Managing Cybersecurity Risk For Government Contractors

Government Technology & Services Coalition
Dickstein Shapiro LLP
October 2013

An Overview Of The Risk

Data Breaches/Cyber Attacks

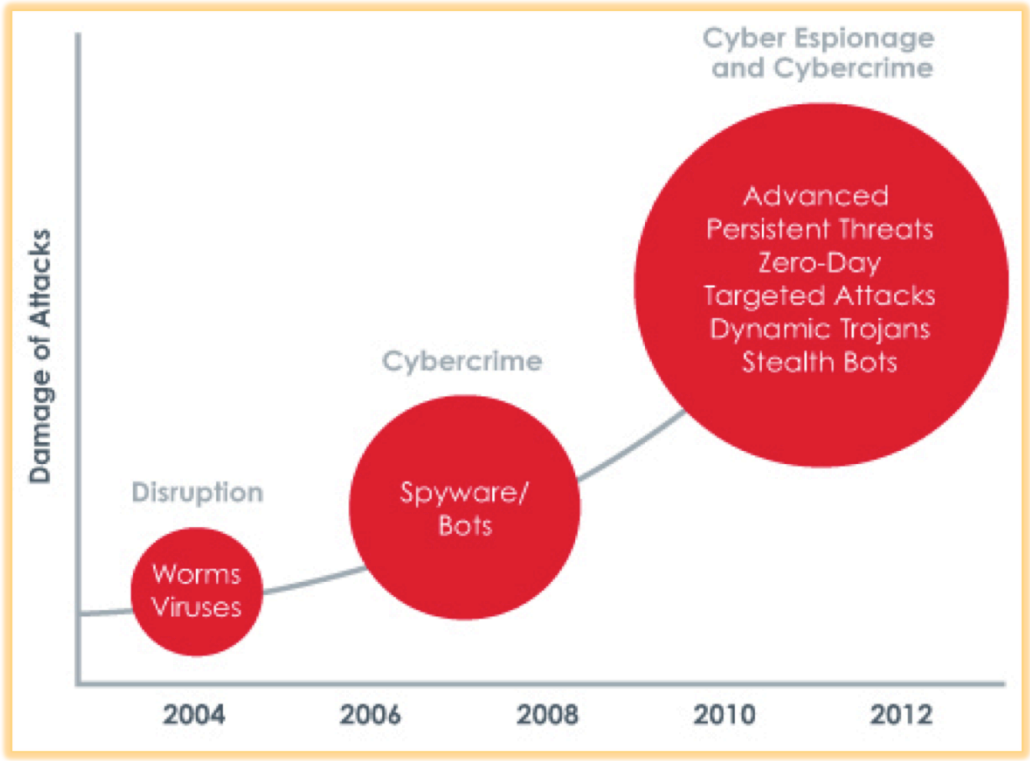
- Exposure of corporate secrets, trade secrets, and other proprietary information.
- Exposure of personally identifiable information.
- Disruption/Destruction of Operations.
- Impermissible use or disclosure of protected health information.
- Cost of an attack may be minimal ($2 for DDoS; $5000 for “zero day”) .

GTSC

DICKSTEINSHAPIRO LLP

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.



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

GTSC

DICKSTEINSHAPIRO LLP

Large Scale Breach Lessons Learned

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	30%
Executive compensation	30%
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 1,957 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.

Figure 1
Top 10 concerns for directors and general counsel:

Directors	
★ Data security	48%
Operational risk	40%
Company reputation	40%
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%

CORPORATE BOARD MEMBER®
An NYSE Euronext Company

2012 SPECIAL SUPPLEMENT

GTSC

DICKSTEINSHAPIROLLP

But I'm Too Small To Be Hacked …

The New York Times
nytimes.com

Hacking U.S. Secrets, Chinese Pushes For Drones

9/20/13

"Though the initial victims in Operation Beebus were large defense contractors, **the hackers began to pick out companies that specialized in drone technology**, said Mr. Kindlund, FireEye's threat intelligence manager. **They then alternated between large companies that made a wide range of military technology and boutique firms that focused on drones."**

GTSC

DICKSTEINSHAPIRO LLP

DoD Will Point Fingers

- **Shifting Sands** – DoD/others shift focus for responsibility *away* from agencies and *toward* contractors:
  - Head of F-35 Lightning II program told Senate Armed Services Committee he worries about the cyber vulnerabilities of "our industry partners." Air Force Lt. Gen. Christopher Bogdan:

"If there are cyber weaknesses related to the F-35, they're on the side of the private sector."

DoD's "robust procedures" keep F-35 data secure within the Department. "I am less confident about our industry partners, to be quite honest with you."

Underlying Framework for Federal Contractors

- Many laws play a role – FISMA, Privacy Act, HIPAA, State Laws.
- FISMA directs federal agencies to develop agency-wide information security programs (does not cover national security systems).
- Standard setting overseen by OMB and NIST.
- OMB says contractors are subject to FISMA requirements.
- NIST's publications set forth key cybersecurity standards:
  - NIST Special Pub. 800-53 – "Recommended Security Controls for Federal Information Systems" (updated April 30, 2013).

Current State of Regulations for Federal Contractors – The Patchwork

- FISMA does not directly impose requirements on contractors, but delegates standard setting to agencies.
- Congress has delayed in passing comprehensive cybersecurity standards (but see 2013 CR language banning Chinese IT system acquisitions).
- Proposed FAR and DFARS rules not yet finalized, though contractors should anticipate safeguarding and reporting requirements in any final rules.
- This has led to a patchwork of regulations, directives, and guidance that vary by agency.

Some Current Regulations/Guidance

Already-effective changes to GSA Acquisition Manual (GSAM). GSAM 552.239-71.

- IT Security Plan.
- Security Authorization.
- Notice and Access.

Other agencies have also established new cybersecurity regulations under FISMA:

- DOD: DFARS 204.404-70(a); DFARS 252.204-7000.
- DHS: HHSAR 339.7103; HHSAR 352.239-72.
- DOE: DEAR 904.404(d)(7); DEAR 952.204-77.
- NASA: NFS 1804.470-3; 1804.470-4; and 1852.204-76
- VA: VAAR 839.201; VAAR 852.273-75.

Cyber Requirements for Cleared Defense Contractors

- Section 941 of the 2013 NDAA imposes disclosure requirements:
  - "Cleared Defense Contractors" have to "rapidly" report to DoD any time they suffer a network or information system "penetration".
  - Security audits – DoD can inspect systems as they see fit.
  - Procedures TBD (DFARS Case 2013-D018).
- Open questions:
  - What is a penetration?
  - Will investigations be disclosed?
  - Is this a "material" event?
  - Will this extend to unclassified networks?
  - Impact on trade secrets / sensitive data?

GTSC

DICKSTEINSHAPIRO LLP

More DOD Requirements

- DOD Updates 8500 Series Guidance.
- Previously just addressed cybersecurity for communications systems.
- New changes to be debuted in October will extend far beyond that:
  - Industrial Control Systems (energy, water, air conditioning, physical security controls, etc.).
- DOD believes there are "cybersecurity implications" for anything connected to its networks, and so cybersecurity controls will be imposed on those connections and underlying systems.
- "In line" with private sector expectations, according to DOD.
- Bottom line – expect more cybersecurity requirements for any system linked to DOD.

Executive Order 13636 – An Attempt at Standardization

- EO 13636 focuses on **two categories of cybersecurity**:
  - (1) Information sharing.
  - (2) Protection of privately held critical infrastructure.
- **Section 8(e).**
  - DoD and GSA will recommend security standards in acquisition and contracting practices, including the harmonization of cybersecurity requirements.
- **DoD and GSA established the Section 8(e) working group.** Draft RFI seeks input on feasibility of new requirements and current commercial practices.
- NIST recently published a draft framework for the protection of critical infrastructure.
  - Identify, Protect, Detect, Respond, Recover.

Recommendations of GSA Working Group

- "Entire federal acquisition spend" should be (1) categorized, (2) assessed for cybersecurity risk, and (3) prioritized according to risk, essential functions, and agency mission;
- Agencies should require cybersecurity assessments for all acquisitions *early* in the requirements definition phase;
- Acquisitions should have cybersecurity concurrence/approval prior to issuing the solicitation and prior to contract award;
- Acquisitions should have cybersecurity approval/review of contractor performance during contract administration;
- A common lexicon should be developed for use in acquisitions related to cybersecurity (or is it cyber security?); and
- A common, but role-focused, training program should be developed for acquisition stakeholders.

Offline GSA/DOD Comments On Procurements

- GSA is looking to set “boundaries” or “lanes” related to cybersecurity in procurements;
- Not *every* procurement is going to consider cybersecurity, but many will;
- Cybersecurity measures could constitute threshold requirements;
- GSA, DOD, and all other agencies are taking this extremely seriously.

GTSC

DICKSTEINSHAPIROLLP

Implications and Risks of the Patchwork

- Many compliance requirements to track and follow (at both agency and procurement level) – risks of non-compliance;
- Protests related to eligibility conditions;
- Potential for False Claims Act litigation for violation of cybersecurity requirements;
  - Implied certification theory and expansion of FCA increases litigation risks.
- Increase in cyber-audits and reporting requirements.

What Should Federal Contractors Do Now?

- Formalize central oversight of cybersecurity issues (regulatory compliance, security, reporting, risk management, etc.);
- Review and assess your current practices for both cleared and non-cleared systems;
- Review your current obligations under prime and subcontracts (and address any gaps);
- Assess risk management/risk transfer (SAFETY Act, insurance coverage, indemnities, PR).

5 Steps for the resource-constrained:

- Make sure you have current security software and that it is updated regularly;
- Make sure computers are physically secure (e.g., locks on laptops, passwords on all terminals, mobile devices, and computers);
- Train your people!;
- Consider a cyber audit/gap analysis;
- Assess risk management/risk transfer (SAFETY Act, insurance coverage, indemnities, PR).

Risk Transfer: The SAFETY Act

"**S**upport **A**nti-Terrorism by **F**ostering **E**ffective **T**echnologies Act"

- Part of the Homeland Security Act of 2002.
- **Eliminates** or minimizes tort liability for sellers of DHS-approved cyber security technologies should suits arise after a cyber attack, including:
  - SAFETY Act protections can be obtained only by submitting an application to DHS.
  - *Applies to services, products, policies, and self-deployed programs.*
  - Protections apply even if approved technologies are sold to **commercial** customers or if act of terror occurs **abroad** so long as US interests implicated (i.e., economic losses).

GTSC

DICKSTEINSHAPIRO LLP

Cyber Attacks Trigger SAFETY Act Protections

SAFETY Act applies to any attack that is:

- (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.

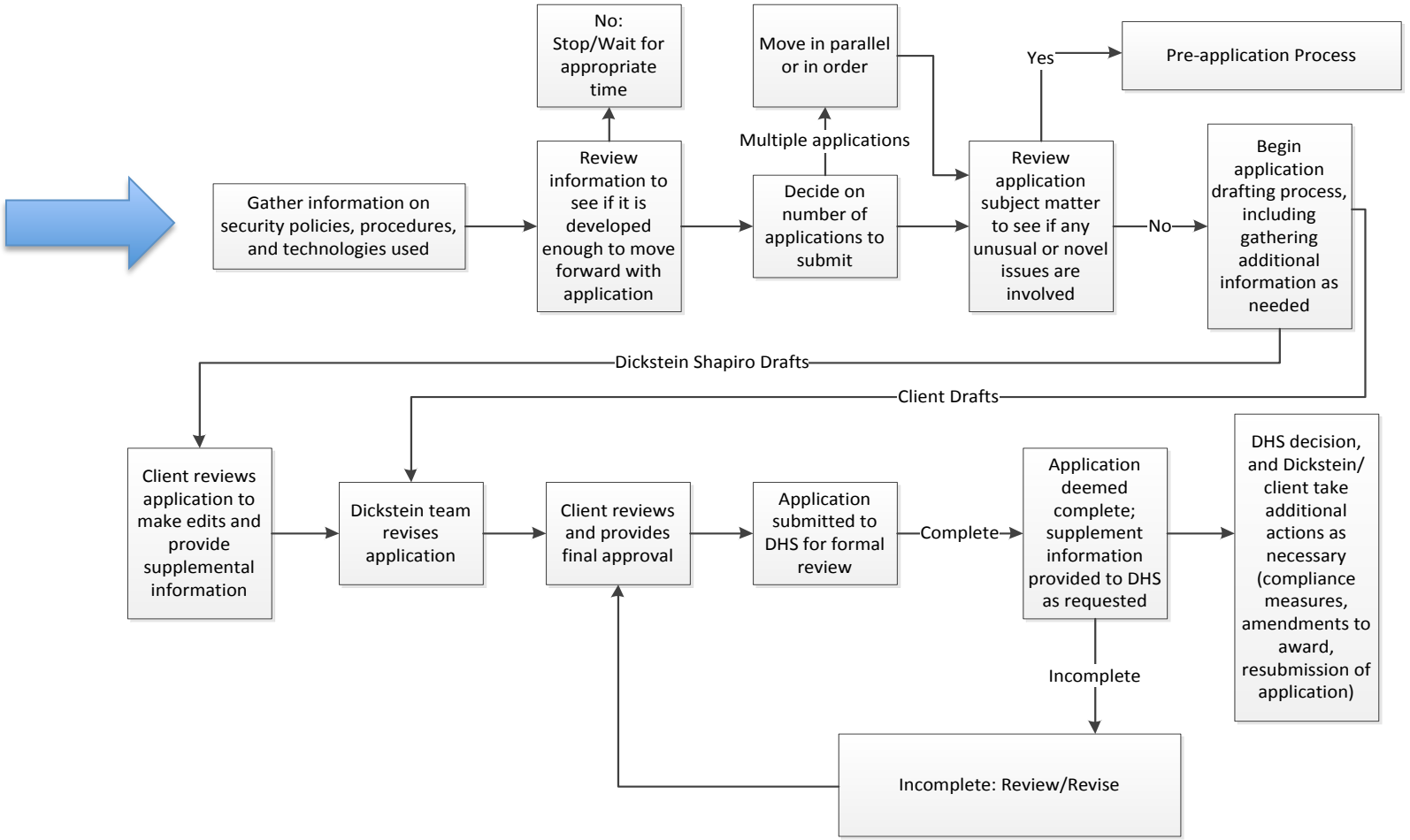
Act of Terrorism = Cyber Attack

- 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.

SAFETY Act: Designation Vs. Certification

- Two levels of protection under the SAFETY Act.
- 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.
- Under "Certification" sellers also receive a presumption of immediate dismissal.
- In both circumstances claims against **CUSTOMERS are to be immediately dismissed**.

The Application Process



GTSC

DICKSTEINSHAPIRO LLP

Insurance Coverage Issues

Emphasis On Cyber Risk Management

Concerned but Not Prepared for Cyber Risks

65%
public companies surveyed that do not purchase cyber insurance

63%
decision-makers concerned about cyber risk

57%
companies that do not include cyber-liability insurance as part of a security breach plan

Source: Chubb 2012 Public Company Risk Survey

Growing Recognition of Cyber Threats

AIG Survey of 258 Business Execs

Risks that respondents are "very or somewhat concerned" about:

Cyber risks	85%
Income loss	82%
Property damage	80%
Securities and investment risk	76%

Source: AIG

GTSC

DICKSTEINSHAPIRO LLP

What Is "Relevant Insurance Coverage?"

- May include:
  - Cyber insurance
  - "Traditional" insurance policies
  - Additional insured coverage
- Insurers *and* brokers are promoting the misconception that new "cyber" product offerings demonstrate the lack of coverage under traditional insurance policies. But traditional policies may still provide substantial coverage pursuant to their plain language.

GTSC

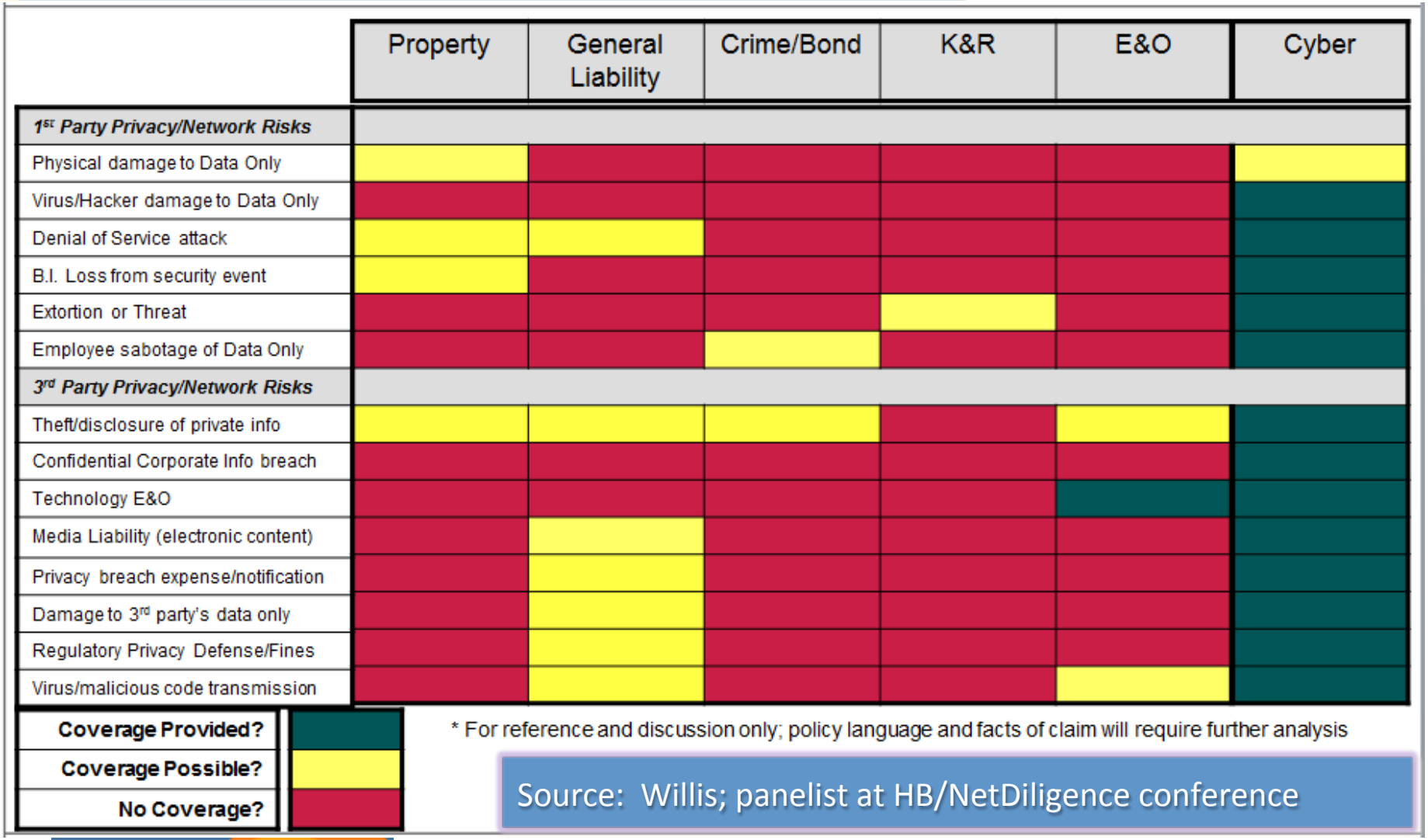
DICKSTEINSHAPIRO LLP

Cyber Insurance Policies

- "Cyber" coverage is the "wild west" of insurance. The market is evolving rapidly; after initial reluctance to insure cyber at all.
- No standard form policies. Policy language varies insurer by insurer and year by year. Most policies have yet to be tested in court.
- Premiums also vary, with most insureds purchasing between $5-$20M in limits.
- Coverage may also be contingent on adherence to certain technical data/system requirements.

27

Cyber Insurance Policies: Marketed As Filling The Gaps Under Traditional Insurance Policies



Source: Willis; panelist at HB/NetDiligence conference

28

GTSC

DICKSTEINSHAPIRO LLP

Other Potential Sources of Coverage: Indemnity Agreements and Additional Insured Coverage

- Review agreements with contractors and vendors to determine where they include indemnity provisions broad enough to encompass losses and liabilities resulting from cyber risks.
- Determine whether you may be covered as an additional insured under policies purchased by contractors and vendors.

Key Contacts

Kristina Tanasichuk– Chair & CEO – GTSC
ktanasichuk@GTSCoalition.com | 703.201.7198

Justin Chiarodo – Partner – Dickstein Shapiro
chiarodoj@dicksteinshapiro.com | 202.420.2706

Brian Finch – Partner – Dickstein Shapiro
finchb@dicksteinshapiro.com | 202.420.4283

GTSC

DICKSTEINSHAPIROLLP