Today we are going to look at cyber risk issues – specifically as they apply to the Supply Chain and more importantly YOU!

Before we start I want to hit a few items as I think they will help our discussions:

1. What is Cyber Security / Cyber Risk?

   Basically it is anything and everything that is associated with the security and/or integrity of or Risk (R = (T X V) I) associated with the 1's and 0's in your environment.

   VERY BROAD – Very Interrelated

2. Does this apply to me?

   (Bell shaped curve) explain normal distribution

   That said, if you are associated with the supply chain – This applies to you.

Speaker Bios:

Tim Hall, President of AZORCA Cyber Security, LLC brings 30 years of experience developing and integrating information assurance and cyber security solutions into complex commercial and government classified systems. He currently provides a broad range of cyber security consulting services to commercial business and government contractors focusing on cyber related supply chain and enterprise risk management.

Prior to forming AZORCA Cyber Security, LLC, as a Booz Allen Hamilton Vice President, Tim led the Cyber Technology team in the civil finance market; providing IT Infrastructure, Cyber Security and Cyber Risk Management support to federal finance clients. Tim also led Booz Allen's Information Assurance and Cyber Security practitioners delivering a broad range of capabilities to the National Security Agency's (NSA) Information Assurance Directorate (IAD).

Tim holds a BS, MBA and five patents in the areas of communications security and information assurance.

++

J. Dino Almendral is the owner and founder of JDA Solutions, LLC. Dino has more than 25 years of experience providing legal and management advice to commercial companies and government agencies. His company provides Governance, Risk Management, and Compliance consulting services to corporate clients and has expertise in such areas as Contract Management, Intellectual Property, and Global Trade.

Prior to his current position, Dino served as corporate counsel for several companies including General Dynamics, BAE Systems, and The Boeing Company.

Dino holds a BA from the University of Chicago and a JD from New York Law School. He is licensed to practice law in New York, New Jersey, Idaho, and New Mexico.

++

Jennifer Bisceglie is an award-winning business owner of a multi-million dollar supply chain and logistics company that helps create comprehensive cyber, supply chain risk management process and technology

solutions for numerous government agencies and commercial entities. Prior to founding Interos, Jennifer honed her 20 years of supply chain management experience in software companies and global distribution companies such as Manhattan Associates, Nine West Shoes (now Jones Apparel), and American Eagle Outfitters.

In 2005, Jennifer launched Interos to deliver comprehensive supply chain solutions to federal agencies looking to mitigate their supply chain risk and enable them to conduct business as effectively as possible.

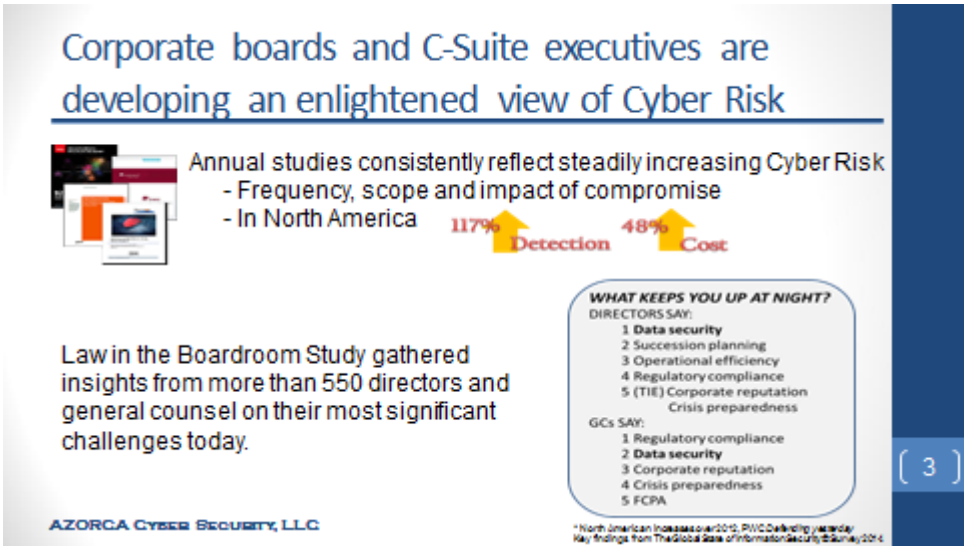
Interos Solutions (Interos) is a supply chain risk management consulting firm providing a broad range of technical services, including enterprise information technology solutions (IT), Cybersecurity and Supply Chain Risk Management (SCRM), network security, integrated logistics support (ILS) systems engineering, modeling & simulation and training/education. Interos has worked with a number of public and private sectors companies in various industries ranging from technology and telecom to medical devices and pharmaceuticals.

++
Objectives: Cyber security and cyber risk are becoming common place and top of mind issues. There is even a CSI *Cyber* on prime time TV. The reality is that despite all the hype it is a serious problem that directly affects the supply chain practitioner. Most of the discussions regarding cyber risk paint a very bleak picture. This is followed by recommendations for significant actions e.g., complete enterprise assessments, penetration testing, acquisition of security tools and systems. With typically high costs to implement these types of activities, it is virtually impossible to fit them into the existing budgets, priorities and schedules. As a result nothing happens.

Our objective today is to discuss how facets of cyber risk present themselves in the supply chain and to give you practical steps you can take, within your current budgetary and operational constrains, to materially reduce your overall enterprise risk position.

There is a lot of talk at these conferences about raising the stature of the supply chain professional within the organization. This is a perfect opportunity for these professionals to contribute at the enterprise level to reduce the overall enterprise risk profile and (if done right) enhance the profitability and competitive position of the enterprise within in market. The best analogy is to compare cyber risk to Quality. Proactively embracing quality has proven to raise profitability, enhance competitive position and assist in partnering and product development / enhancements.

Take-aways: You cannot stop a determined adversary. You can be prepared to respond and minimize the pain. This will also make recovery from cyber based disruptions more forecastable.



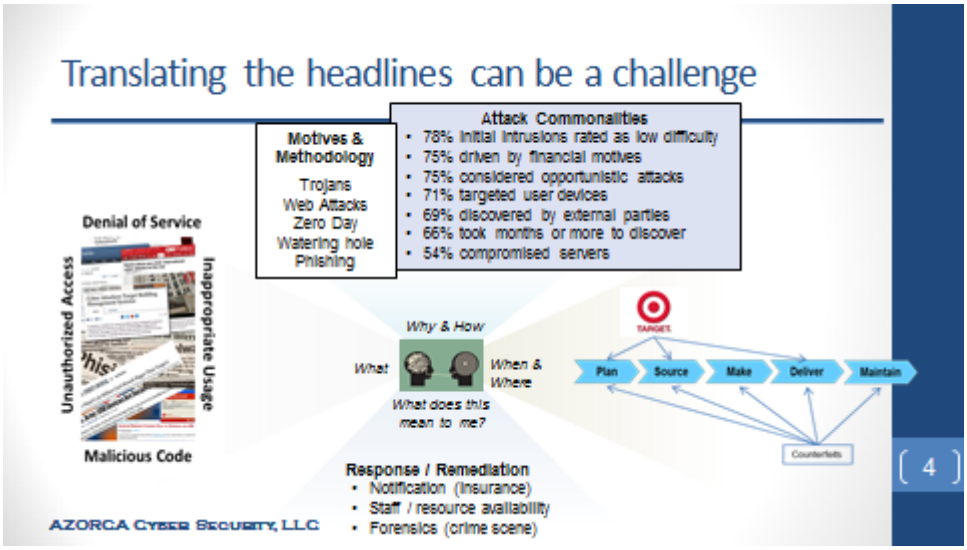
The good news is cyber security / cyber threat is becoming recognized at the board and C-Suite as a critical item and as a serious risk that really applies to them.
No wonder since the Target CEO and CIO wire fired and there was a motion to remove the entire board in response to the breach.
The Law in the Boardroom Study is conducted by FTI Consulting annually. Yet when C-level leaders are asked; 74% say their security activities are effective, 84% of CEO's say they are confident in their security programs and 78% of CISOs report confidence in their programs. Finally, 80% of leaders say their security spending is in line with their business objectives. This is in stark contrast to the PWC study *"PWC Defending Yesterday, Key findings from The Global State of Information Security® Survey 2014"* that indicated that three of the top four **obstacles**, cited by C-Suite respondent, to improving information security were:

- Lack of actionable vision or understanding of how future business needs impact information security
- Leadership: CEO, President, Board or equivalent
- Lack of effective information security strategy

Clearly there is confusion regarding the state of affairs and how to deal with it.

The traditional reactive approach to information security strategy, which typically relegates security to an IT challenge, remains commonplace. This is no longer effective, nor is it defensible **especially in light of evolving cyber threats and guidance and regulatory trends.**

Organizations must treat information security threats as enterprise risk-management issues that can critically threaten business objectives. Safeguarding *all data* at the highest level is no longer realistic or even possible.



Translating the headlines into meaningful and actionable plans can be a challenge for the non-cyber skilled business manager.

The headlines talk about cyber breaches, data leaks, worms, virues, trojans, Distributed Denial of Service attacks (DDoS), HeartBleed, Stuxnet, counterfeits, taints, credit card thefts and loss of Personally Identifying Information (PII) and Private Health Information (PHI).

What exactly are these? How are they related? Should I realistically be concerned about all of them?

What if I am small business? How do I address comments like: What I make is not important. I do not have PII or credit card info associated with my supply chain.

Where do these risks manifest themselves in the supply chain? Can I reasonably forecast or at least prioritize my expectations?

Most user's knowledge of cyber risk its potential impact comes from what they learn via the news. Most news reports recount losses of PII, or credit card information. Much of the impact cited in the articles refers to breach notification laws / requirements and individual's potential identity theft. While this is a significant issue, it is only one facet of the problem. The business headlines are not quick to highlight less sensational but potentially equally damaging cyber events that have a direct impact on the supply chain but might not trigger breach notification requirements. For example:

- Counterfeit or tainted components
- Ransomeware
- Compromising the supply chain to gain access to the ultimate target --- example HVAC supplier and Target
- DDoS attacks – supplier disruption
- IP theft
- Web / watering hole attacks

Attacks:

The objectives of most attacks are to compromise an individual's system to:

1. Steal the content
2. Subvert operation or control

3. Leverage the platform to elevate privileges to move horizontally throughout the system to the desired endpoint.

Attacks are directed at an individuals or at a website, product or component that individuals would use as a way to access the targets.

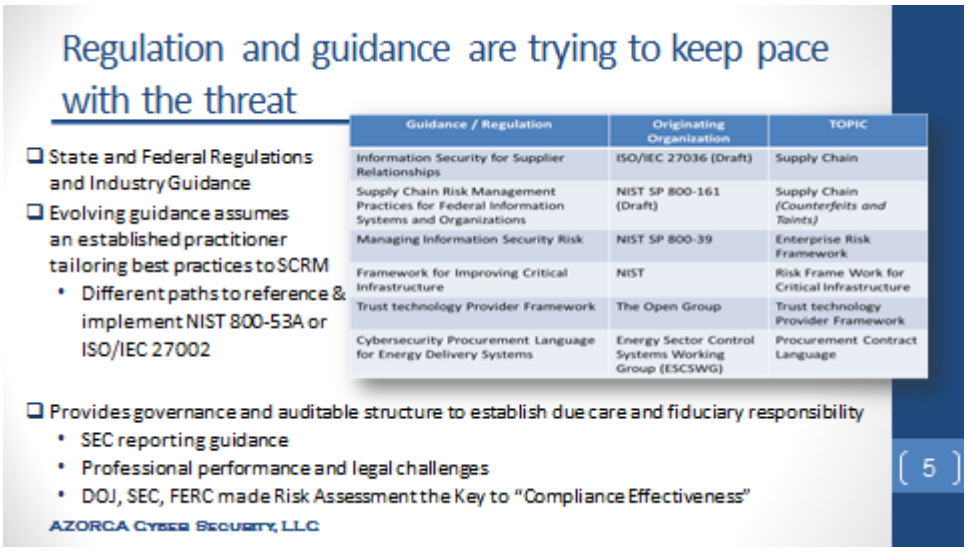
Attack approaches

1. Broad network attacks – These are really targets of opportunity attacks. They do not discriminate. They have the potential to compromise anyone / any organization regardless of size or sophistication (see gray insert box on the slide).
    - Phishing, worms, viruses, trojans, ransomeware.
    - These will compromise a system, open a backdoor to enable theft and exfiltration of data or enable the attacker to re-purpose the assets as botnets, etc.
2. Intermediate type attacks. Attacking systems that your type of target would normally use e.g., Watering Hole Attacks – attacks to a website where people (the type that are being targeted typically go). You trust the site, so you click on the links and download malware. Then it is the same problem as above.
3. Direct attacks
    - Leverage social engineering
    - Spear phishing
    - Unique malware
    - Usually looking for longer term or more substantial compromise e.g., long term theft of IP and competitive information or Home Dept, JP Morgan, Target type compromise.

Number 1 and 2 can affect anyone. Number three can be directed even at a small company to gain access to a larger target.

Response and Remediation is generally much more than you think.

To be able to forecast and plan for the response and remediation you have to be able to anticipate the vulnerabilities, threats and understand the full scope of activity required for response and remediation. IT IS NOT JUST NOTIFICATION. There are increased IT staff requirements, log reviews, system analysis, forensics analysis, regulatory reporting, communications, contractual liabilities, operational and system disruptions, legal liabilities, eDiscovery, etc. You need support (personnel resources) to complete all of the above and you need it immediately.



Governing bodies are aggressively pursuing laws, regulations and guidance to stem the tide of increasing cyber activity and resultant risk.

The growing recognition of broad based supply chain cyber risk is driving the development of "Guidance" documents (e.g., Cyber Security Procurement Language for Energy Delivery Systems, NIST SP 800-161 Supply Chain Risk Management 5 Practices for Federal Information Systems and Organizations, Trust Technology Provider Framework and ISO/IEC 27036 Information Security for Supplier Relationships).

While these guidance documents are developed and intended for a specific target audience (e.g., Energy distribution, US federal agencies, etc.), it should be anticipated that these documents will be used to define best practices, which will become the foundation for legislation and regulation.
In keeping with the historical evolution of regulation and controls, the evolving "Guidance" documents are based on current best practices and controls from current resources NIST, ISO etc. documents. They assume a knowledgeable practitioner with an established baseline.

The challenge is that in the midst of these evolving developments many commercial organizations do not have the practitioners (especially associated with supply chain) nor do they have candid assessment and understanding of their baseline.

It should be noted that audit and compliance frameworks are firming up in advance of many commercial organization's awareness or ability to respond, as seen in the following article.

> In the long-awaited guidance on Foreign Corrupt Practices Act ("FCPA") enforcement, the Department of Justice ("DOJ") and Securities and Exchange Commission ("SEC") unexpectedly articulated the elements of an effective corporate compliance program for detecting and preventing FCPA violations. The guidance was welcomed because FCPA enforcement has been unrelenting with fines moving into the stratosphere. The guidance forcefully provides that effective compliance programs must be tailored to the risks associated with the business and

regulators will give meaningful credit to companies that implement risk-based programs. A similar message was conveyed by the Federal Energy Regulatory Commission ("FERC"), which was recently reinforced in an order directing Barclays Bank PLC to show cause why it should not be required to pay nearly a half-billion dollars in civil and other penalties for alleged manipulation of electricity markets in and around California. A Resource Guide to the U.S. Foreign Corrupt Practices Act (Nov. 14, 2012), available at <http://www.sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf>.

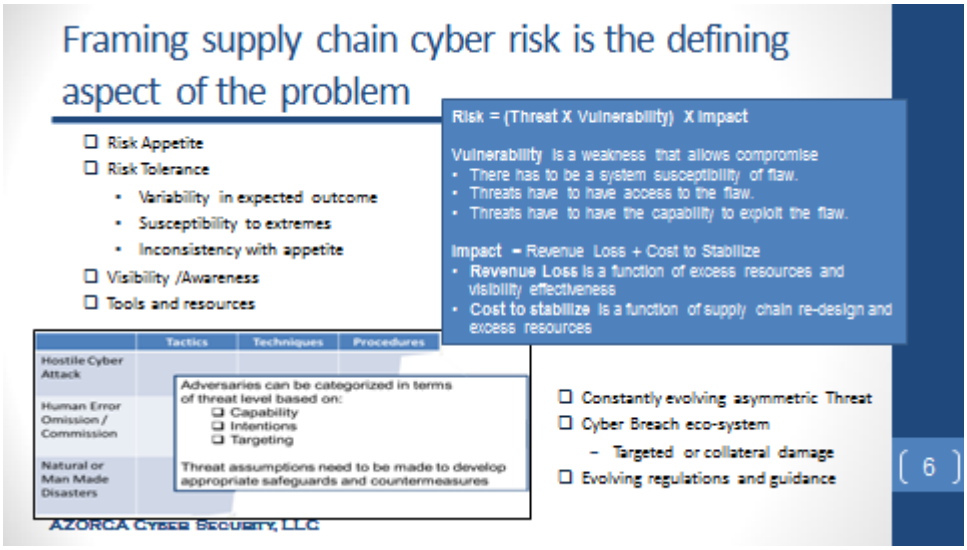
Barclays Bank PLC et al., 141 FERC ¶ 61,084 (2012).

The DOJ, SEC, FERC and other regulatory bodies have articulated leniency standards for companies that have implemented effective compliance procedures. Even if regulators do not have leniency programs, the standards for effective compliance programs have become "best practices" in corporate America because they enable a company to self-police its conduct by identifying, assessing and correcting compliance problems before they are discovered by regulators.

Effective compliance programs are grounded on a company's periodic assessment of risks. This premise underpins the compliance standards delineated in the Federal Sentencing Guidelines, the recent DOJ/SEC guidance and other federal regulatory guidelines. U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(c) (2004).

The compliance program standards delineated in the Sentencing Guidelines have become the gold standard for measuring the effectiveness of compliance programs. While these standards are not mandatory, most organizations follow them because regulators (including the DOJ, SEC and FERC) use them in making decisions about whether to prosecute a compliance violation or recommend leniency. The standards have become "best practices" in corporate America because they enable organizations to self-police their conduct by identifying, assessing, and correcting compliance problems before they are discovered by regulators.

Further, the Sentencing Guidelines provide that a company's failure to incorporate and follow applicable industry compliance practices weigh against a finding of an effective compliance program. With that in mind, companies should consider forming compliance best practices groups to share information on industry compliance risks and best practices for achieving industry regulatory requirements.



Due to the depth, breadth, and technological half-life of the cyber environment, framing Supply Chain Cyber Risk, is difficult for a tenured practitioner:

Establishing assumptions: Criticality, Threats, Vulnerabilities, Impact, Likelihood
Identifying constraints
Establishing risk tolerance
Establishing priorities
Identifying trade-offs

The risk position can change substantially depending on where you are in the larger supply chain and who your suppliers are. The same holds true for your suppliers. Yet it is surprising that as more organizations open their networks, applications, and data to third parties:

- Only 20% say they evaluate more than once a year the security of third parties with which they share data or network access. Indeed, 22% say they do not evaluate third parties at all, while 35% say they evaluate third parties once a year or less. Similarly, only 22% of respondents say they conduct incident response planning with third-party supply chain partners, while 52% never conduct incident-response planning for third party supply chains.
- (24%) respondents say they will implement security standards for external partners, suppliers, vendors, and customers.

Properly framing the risk requires that you can identify system flaws that can realistically be compromised and that an attacker can access and falls outside your risk appetite. Additionally, the practitioner needs to effectively understand the threat which includes an appreciation for their motives, attack methodology and capabilities so that you can estimate their ability to leverage a system flaw. Finally you need to be able to scope the associated response and remediation requirements to be able to estimate the impact. Most cyber victims underestimate the response and remediation activities following a cyber event. Response and remediation is much more than notification. There is generally an immediate demand for staff resources to support network and data analysis, forensics, system recovery, eDiscovery, etc not to mention support for communications, internal management and coordination and legal action.

Supply Chain Risk Includes:

- Availability
- Intellectual property
- Financial
- Privacy
- Counterfeits and taints
- Legal and regulatory
- Reputational

What are supply chain risks? How big of an impact? How likely to occur?

Depends on:

- Where in the supply chain you reside
- What you consume and what you offer
- Who do you consume from and who do you sell to
- Your current cyber security profile and capability

Supplier integration, advanced analytics and evolving IT applications are critical for maintaining a competitive supply chain. These advancements increase the cyber-attack surface and impact the enterprise risk position. Threats to the Critical Infrastructure, shareholder value and consumers are driving the development of regulation and guidance that will have increasing impact on ***SCRM liability and audit trends are likely to expand reporting requirements and the applicability of the standards and guidance.***

This brings an additional potential risk; a reporting risk and a "due care" liability risk resulting from requirements and baselines established in the evolving standards and guidance.

Audit and Liability Trends:

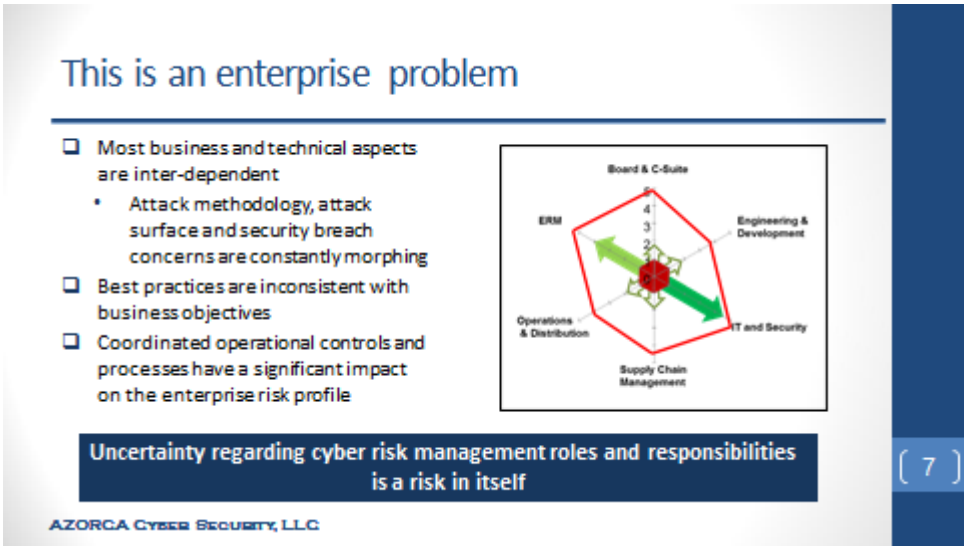
Prior to the guidance from the Division of Corporation Finance of the Securities and Exchange Commission, there were no guidelines as to when a corporation should publicly disclose the loss of confidential information or disruption to a system caused by a cyber incident even where the incident caused financial losses. It was widely assumed that many companies did not report loss of confidential information or a disruption to their computer system caused by a cyber incident for fear of damaging their reputation with investors, customers, and their employees, and highlighting their vulnerabilities. Now, however, corporations and their managers should aware of the guidelines from the SEC on the disclosure of cyber incidents.

The Division of Corporation Finance of the SEC issued guidance to address the increased risks of registrants associated with cyber security and cyber incidents. According to the guidance, federal securities laws are intended, in part, to elicit "disclosure of timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision." The SEC warned that "[a]lthough no existing disclosure requirement explicitly refers to cyber security risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents" and that such material information is required to be disclosed "when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading." The SEC stated, "as with other operational

and financial risks, registrants should review, on an ongoing basis, the adequacy of their disclosure relating to cyber security risks and cyber incidents."

Although the SEC guidance is not mandatory, the SEC is likely to make certain cyber incident reporting requirements mandatory in the future and corporations should be ready to meet such requirements. Even if no mandatory SEC reporting requirements are forthcoming, at the very least, the guidance provides corporations with the opportunity and to ask internally whether they are doing enough to secure their computer systems.

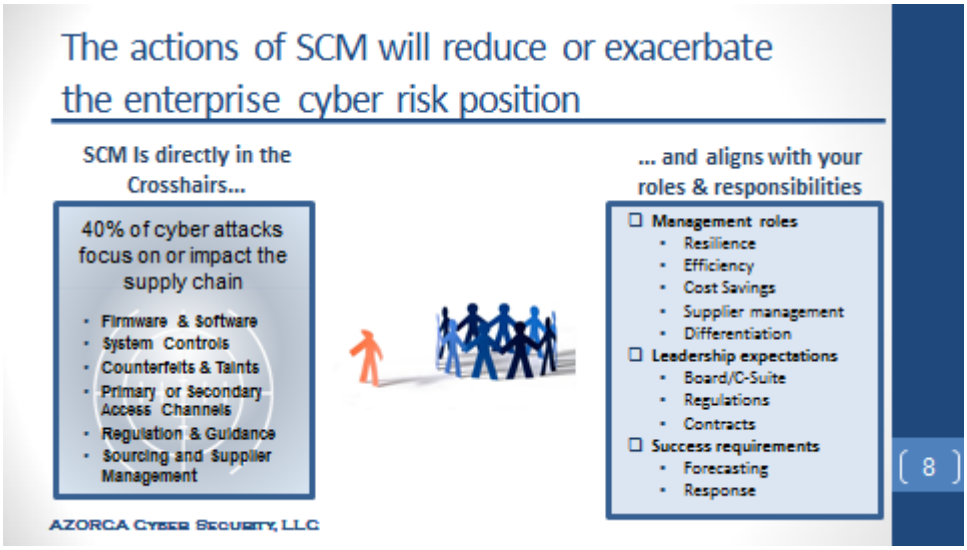
The failure to do so may lead to expensive cyber breaches and having to defend against expensive shareholder lawsuits alleging the failure to take reasonable steps to protect their cyber infrastructure.



Many organizations relegate cyber risk management to CIO, CISO (if one exists) and/or the Enterprise Risk Manager. While one of these positions might be appropriate as the lead, key risk mitigating decisions are controlled by other operational organizations and they need to be an integral part of the cyber risk management function.

Strategic, business and technical system decisions are all interdependent. Active participation is required to ensure information system strategies optimize, and are consistent with supplier / partnering, contractual and information sharing tactical decisions and long term strategies.

As a practical matter, if there are evolving supply chain cyber security guidance / requirements the supply chain leadership is more likely to get word of it than the CIO or CISO. In any event, if the supply chain leadership tried to abdicate the responsibility to track changes to the CIO / CISO, the supply chain leadership is still likely to have to bear the burden because the new regulation and guidance is “Supply Chain” regulation and guidance.



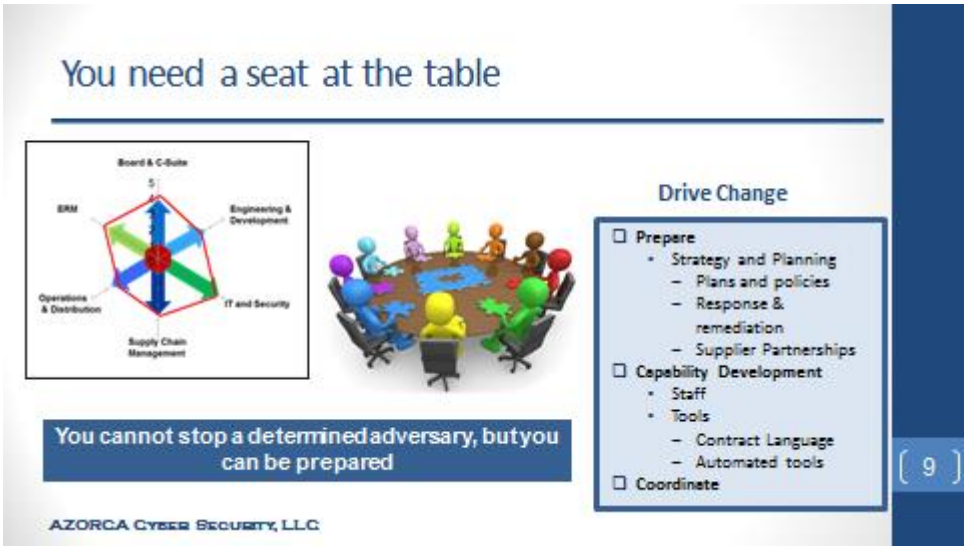
How the supply chain practitioner engages will make a material impact on the cyber risk position of the enterprise as well as the efficiency, cost effectiveness and potential competitive advantage generated.

Sophisticated adversaries recognize the access and value offered by the supply chain. Efforts directed at a facet of the supply chain provide benefits across the entire supply chain. The threats are not only from potential theft and data compromise but also from the ability to disrupt operations.

Not only does this risk management domain align directly with your role and responsibilities, but it is reasonable to anticipate that supply chain cyber risk management, auditing and reporting are likely to flow down from the Board and C-Suite.
Relative to ***Management Role***

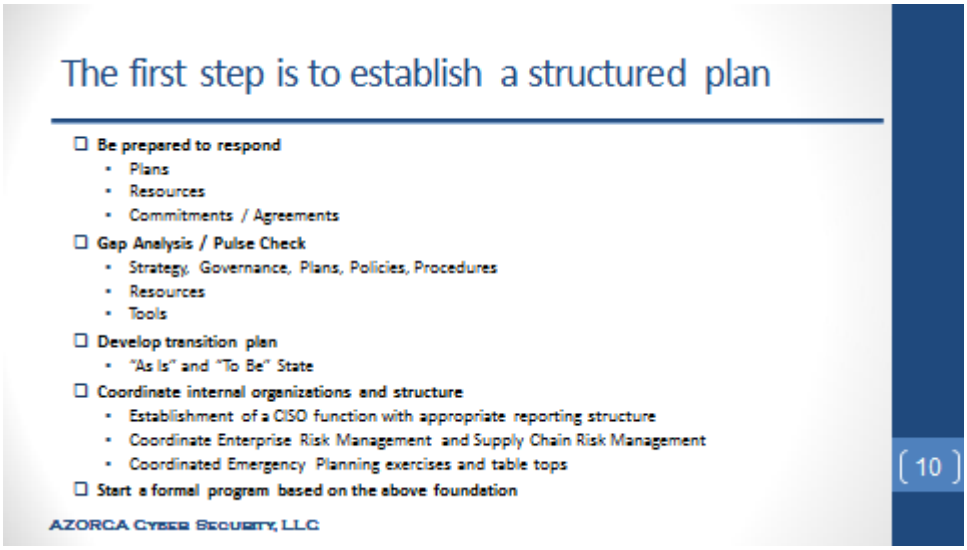
- ***Differentiation***

Discuss the analogy of quality control in the late 80s and 90s. Initially fought, seen as unnecessary burden. Quality evolved to become a differentiator or competitive advantage for the early adopters and then a baseline requirement. Initial quality efforts expanded and evolved to 6 Sigma, Lean, CMMI etc. and drove operational concepts like DFM.



Supply Chain leaders need to have a seat at the table. The supply chain leadership needs to participate in the strategy and trade decisions. To do this, you need to be prepared to participate and have something to offer.

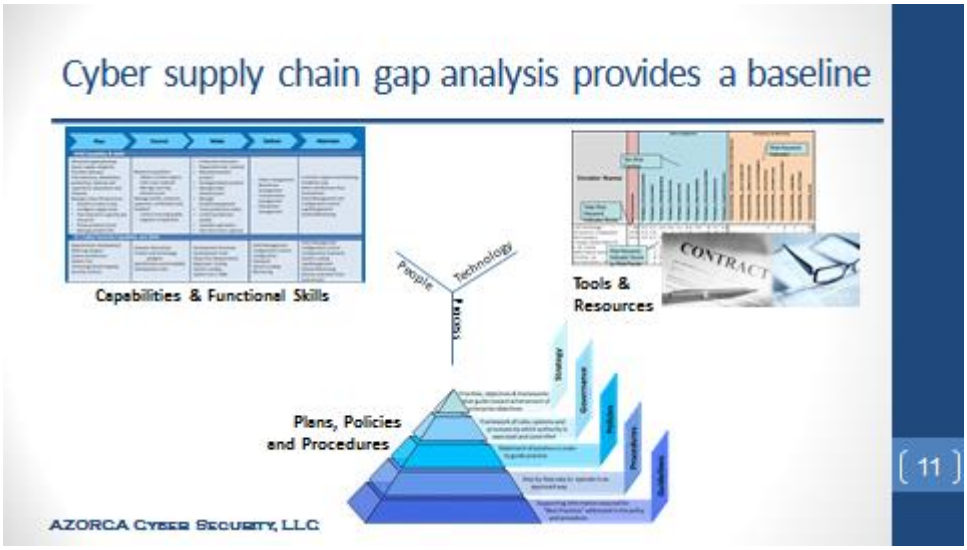
With focused effort in a few select areas you can position the supply chain to be better prepared in the event of a breach. This can be accomplished within your current budgets, schedules and priorities. You cannot stop a determined adversary. But you can be prepared so that you limit the pain and optimize your reputation and competitive position when the inevitable breach occurs **(remember, we are talking about a breach to you or someone up or down your supply chain).**



First order of battle is to be prepared to respond.

A simple gap analysis will let you know where you stand. This will be a big help when you are at the table. You will be better able to discuss vulnerabilities, exposure and potential impact. This will enable better near term trade decisions and long term strategy, budget and planning. Additionally, response preparation could help defend against "due care" concerns.

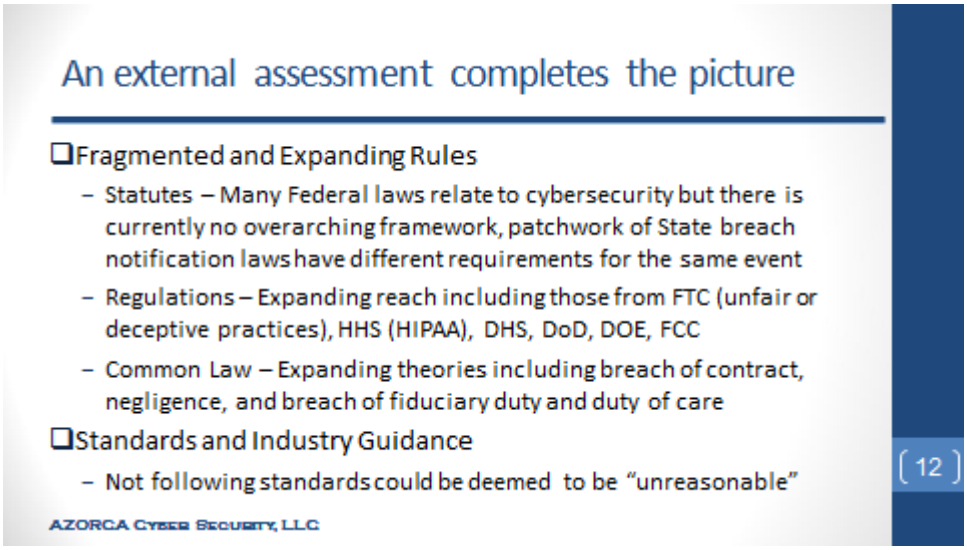
When thinking of tools, think broadly, there are some tools e.g., contract language, contract triage process etc. that will have little to no incremental cost.



Following the classic analysis process, the initial gap analysis process should follow evaluation of People, Processes and Technology. The biggest near term impact at the lowest cost would be to focus on staff functional capabilities, current plans, policies and procedures and available tools.

This is basically an internal assessment.

It is interesting when you map the capabilities, roles and responsibilities of Supply Chain practitioners across the supply chain against IT / Cyber Security professionals across a comparable life cycle there are no overlaps. It is important to have cyber tech staff participating in your planning but that is not enough. ***You need to have supply chain practitioners with cyber security awareness so they can translate the two domains to coordinate processes, priorities and partnership structures and information sharing with third parties.***



Fragmented and Expanding Rules

1. Many laws are already on the books and more are on the way. These laws can overlap and be inconsistent.

2. Different government agencies are expanding the applicability of laws relating to cybersecurity liability through regulations. Existing laws that had nothing to do with cyber liability when they were passed are now being interpreted to impose liability for cybersecurity incidents.

3. Judges in court cases are expanding liability for cybersecurity incidents to theories of law that historically provided no recourse

Standards and Industry Guidance

1. You should be looking at your company, industry, and supply chain to see which standards apply to you either directly (by law, regulation, or express contractual requirements) or indirectly (under common law).

Main Take-Away

If you are not routinely assessing your potential liability for cybersecurity incidents, you probably do not fully appreciate your risk exposure and may be unprepared to adequately respond in the event of an incident. An ounce of prevention may be worth a pound of cure.

There is a broad range of levers available to address cyber security risk, but for the average company there are a number of actions with a relatively small cost, schedule, priority impact that can make a material difference to the supply chain and the enterprise. The recommended primary targets are circled in red.

Discuss what should be done and why it pays disproportionate dividends.

The actual Policies Processes and Procedure needed are defined by the organizational objectives, threat, vulnerabilities and enterprise /supplier capabilities. The actual Plans, Policies and Procedures need to be defined and tailored for each organization. The slide references the policies plans and procedures called out in the NIST Standards. The ones below are examples of actual NIST standards and some of the derivatives.

Access Control
- Password Policy
- Password Construction Guidelines
- Password Protection Policy
- Remote Access
- Bluetooth Baseline Requirements
- Remote Access Tools Policy
- Network Access Policy
- Remote Access Policy
- Guest Access Policy
- Third Party Connection Policy
- Workstation Security (For HIPAA) Policy

Security Awareness and training

Audit and Accountability

Security Assessment and Authorization

Configuration Management
- Retention Policy
- Confidential Data Policy
- Backup Policy
- Information Logging

Contingency Planning

Identification and Authentication
- Digital Signature Acceptance Policy
- Database Credentials Policy
- Incident Response Policy

Disaster Recovery
- Pandemic Response
- Security Response Plan
- System Maintenance

Media Protection
- Acceptable Encryption
- Encryption Policy
- Data Classification Policy

Physical and Environmental
- Physical Security Policy
- Technology Equipment Disposal Policy
- Lab Security Policy

Security Planning

Personnel Security
- Clean Desk Policy
- Ethics Policy

Risk Assessment

System and Services Acquisition
- Acquisition Assessment
- Outsourcing Policy

System and Communications Protection

System and Information Integrity
- Acceptable Use Policy
- Email Policy
- End User Encryption Key Protection
- Router and Switch Security Policy
- Wireless Policy
- Server Security
- Software Installation
- Web Application
- Virtual Private Network (VPN)
- Mobile Device Policy
- Network Security

While this issue / topic (Supply Chain Cyber Risk Management) is continually growing in prominence, training and development programs for the supply chain practitioners on this topic are virtually non-existent. I queried all of the universities exhibiting at the ISM conference and cross checked with the certification programs e.g., CPSM, CSCMP, and found no training or development programs.

Technical cyber proficiency is not the objective. It is important for the supply chain team to have supply chain experts with a cyber sensitivity / awareness so that they can translate between the business / operational objectives and priorities and the IT /Cyber Technical concerns.

There is a lot of talk at these conferences about raising the stature of the supply chain professional within the organization. This is a perfect opportunity for these professionals to contribute at the enterprise level to reduce the overall enterprise risk profile and (if done right) enhance the profitability and competitive position of the enterprise within in market.

There is not a simple or standard set of contract clauses to address all your cyber concerns. Contractual language needs to be tailored based on the materials being acquired, anticipated threat, potential impact, supplier capability / resources and what supply chain strategy you are trying to execute.

Review SLAs to ensure required support will be available in the event of a cyber event.
Outsource services require a different approach than material suppliers and evolving services Cloud, IOT and BYOD may require special attention.

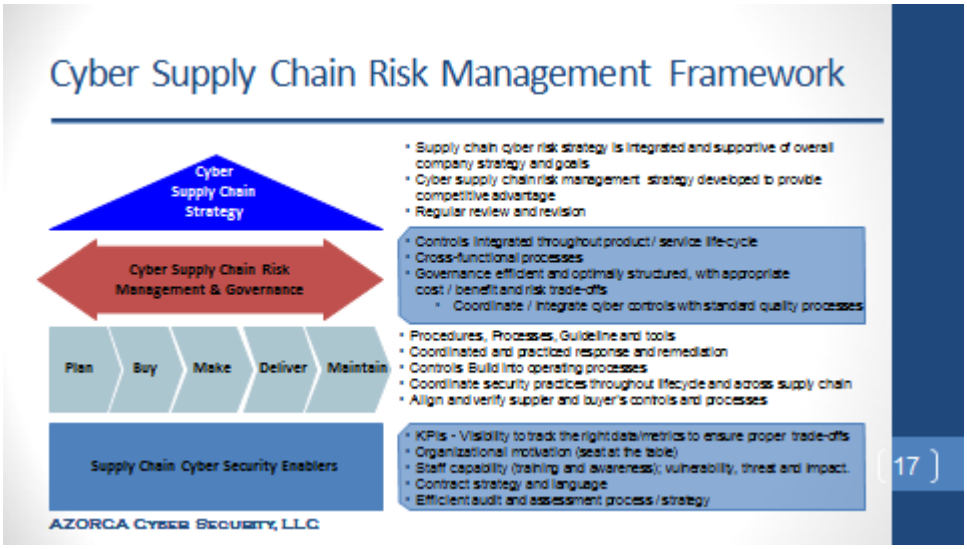
Consider adding specifications and/or requirements to the products and services being delivered by your suppliers to integrate into your operations and leverage your internal processes to help mitigate against cybersecurity risk.

Understand the contract clauses that could relate to cyber liability that are being flowed down to you by your customers and decide whether you must or should flow down the same or similar clauses to your suppliers.

Consider tweaking the standard terms and conditions found in your supplier contracts (e.g., warranties, indemnities, limitations of liability, non-disclosure and disposition of proprietary information, insurance, etc.) to specifically address the allocation of risk for cyber liability.

Main Take-Away
It is good practice to allocate risks based on which party is in the best position to mitigate against such risk. If you are unwilling or unable to take on risks imposed by a customer, you need to evaluate that in light of the overall enterprise risk appetite and risk tolerance. Likewise you need to factor into your supplier selection a supplier's willingness or ability to take on risks you want or need to impose on them.

As a side note it is important to realize that much of the cyber risk cannot be simply addressed with insurance. Discuss the range of risks to be addressed.



Long term success is going to require a well thought out plan based on a framework tailored for the organization, supply chain and projected cyber threats.

Each layer of the framework depends on and flows from the adjacent layers. The framework is tailored / applied as needed in each phase of the supply chain.

Ensure your seat at the table

- ❑Prepare to respond
- ❑Develop your key resources and tools
- ❑Establish a manageable plan