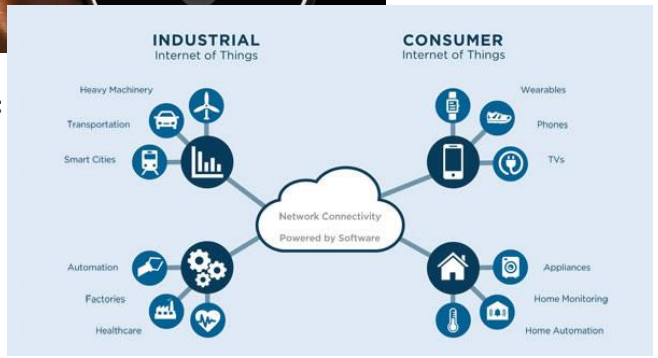
Security Update

April 2017

In the larger world,

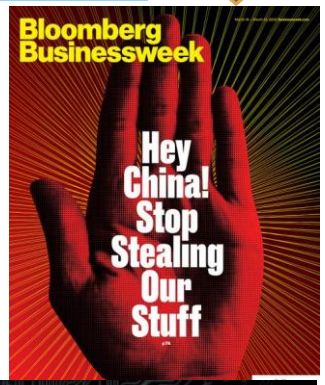
Themes rippling through Information Technology

- Consumerization and mobility is driving … everything
  - Control/Mobile Device Management
  - Control/access to data, personal and corporate
  - Consumer services like gotomypc, Dropbox
- Cloud and Software as a Service (SaaS)
  - Contract terms and conditions - What is where?
  - Authentication and general account management
- Proliferation of the Internet (and Insecurity) of Things (IoT)
  - Vehicles, Smart Homes & TVs, Medical Devices, Embedded Devices…
- Regulatory compliance is more critical – eg, HIPAA



Cyber Security Realities

- Increasingly sophisticated threats
  - Malware, Ransomware, Email spam & phishing, Social Media threats…
  - DDoS, Zero-Day, MitM, “Cloud Hopper”…
- Disappearing Boundaries
  - Actors can locate and attack from anywhere; difficult to trace actors
  - Socially connected networks provide cheap and easy intelligence to plan an attack
- Increasing Risk Adjusted Returns
  - Cost of launching an attack has drastically decreased
  - “Victimless” crime that is “safer” than drug dealing
- Method of Attack Changes Frequently
  - Targeted phishing campaigns to gain login credentials
  - Trusted third-party relationships to bypass controls
  - Malicious insider still concern



- Focus change from protecting the IT infrastructure to managing the information risk to the organization
  - Secure the internal organization
  - Understand and manage the risk of third parties
  - Understand and manage regulatory risks
  - Communicate information risk in business terms

A Layered System of Security Controls

Foundation Controls

- Perimeter (network security):
  - Firewalls
  - Intrusion prevention
- **Access controls:**
  - **User provisioning (role-based)**
  - **Access management (two-factor)**
- Vulnerability management:
  - Patching (45-day cycle)
  - Incident response
- **Security awareness:**
  - **Training (annual)**
  - **Policy**
- Organization:
  - Staff (roles)
  - Skills (certifications)
- Compliance:
  - Audit
  - Requirements management
  - E-discovery

Source - Gartner

Good Controls

- Formal process:
  - Measurable
  - Repeatable
- Detection and Response:
  - **Log analysis (DNS-Level)**
  - User behavior (access logs)
  - Virtual machine scanning
  - Data loss prevention
  - **Across the supply chain**
- Risk assessment:
  - IT risk (applications and projects)
  - Facility risk assessment
  - Automation
- Governance:
  - Governance committees
  - Change management
  - Identity access governance
- Strategic planning

Advanced/Nice to Have

- Business alignment:
  - Integrate controls with business process
- Key risk indicator mapping:
  - Leading indicators of risk that influence business decision making
- Behavior shaping:
  - Reduce technical controls
- Ethical hacking
- Risk management:
  - Enterprise risk
  - Accountability
  - Scenario risk assessment

Information Risk Program

1st Line of Defense IT Information Security	2nd Line of Defense Information Risk Office	3rd Line of Defense Audit and External
Highly Skilled and Trained Staff	Define and Enforce Information Security Policy	Board of Directors Oversight
Processes to Protect, Detect and Respond	Manage Information Risk Program	Internal Audit Validation of Control Framework
Enabling Security Technologies	Program Strategy and Goals	External Audit
	Measure and Manage Information Risk	External Testing and Validation of Controls
	Oversee Industry and Regulatory Requirements	

Breach Impact Financial Liability | Customer Data Protection | Regulatory Risk | Services Availability

Source: Optiv

Fulfilling Fiduciary Duties

"NACD, in conjunction with AIG and the Internet Security Alliance, has identified five steps all corporate boards should consider as they seek to enhance their oversight of cyber risks."

1	*"Directors should approach cybersecurity as an **enterprise-wide risk management issue**, **not just an IT issue**."*
2	*"Directors should **understand** the legal implications of **cyber risk** as they apply to the company's specific circumstances."*
3	*"Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda."*
4	*"Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework."*
5	*"Board-management discussion of cyber risks should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach."*

Source: National Association of Corporate Directors, *Cyber-Risk Oversight Handbook*, 2014.

The Security Function At a Glance

Information Security	**Mandate**: Lead the organization's effort to manage information risk within an appropriate risk appetite.

Key Activities

- ✓ Provide assurance to the Board of Directors that the organization is appropriately managing information risk.
- ✓ Create and maintain information security policies and help set implementation goals.
- ✓ Monitor the threat and regulatory landscapes and identify the top risks facing the organization.
- ✓ Invest in and manage advanced capabilities to improve the protection against and detection of cyber attacks on the organization.
- ✓ Assist risk owners (in the first line of defense) to make risk management tradeoff decisions and select appropriate security controls.
- ✓ Facilitate and monitor the implementation and maintenance of security controls across the organization.

Source: CEB