High performance. Delivered.

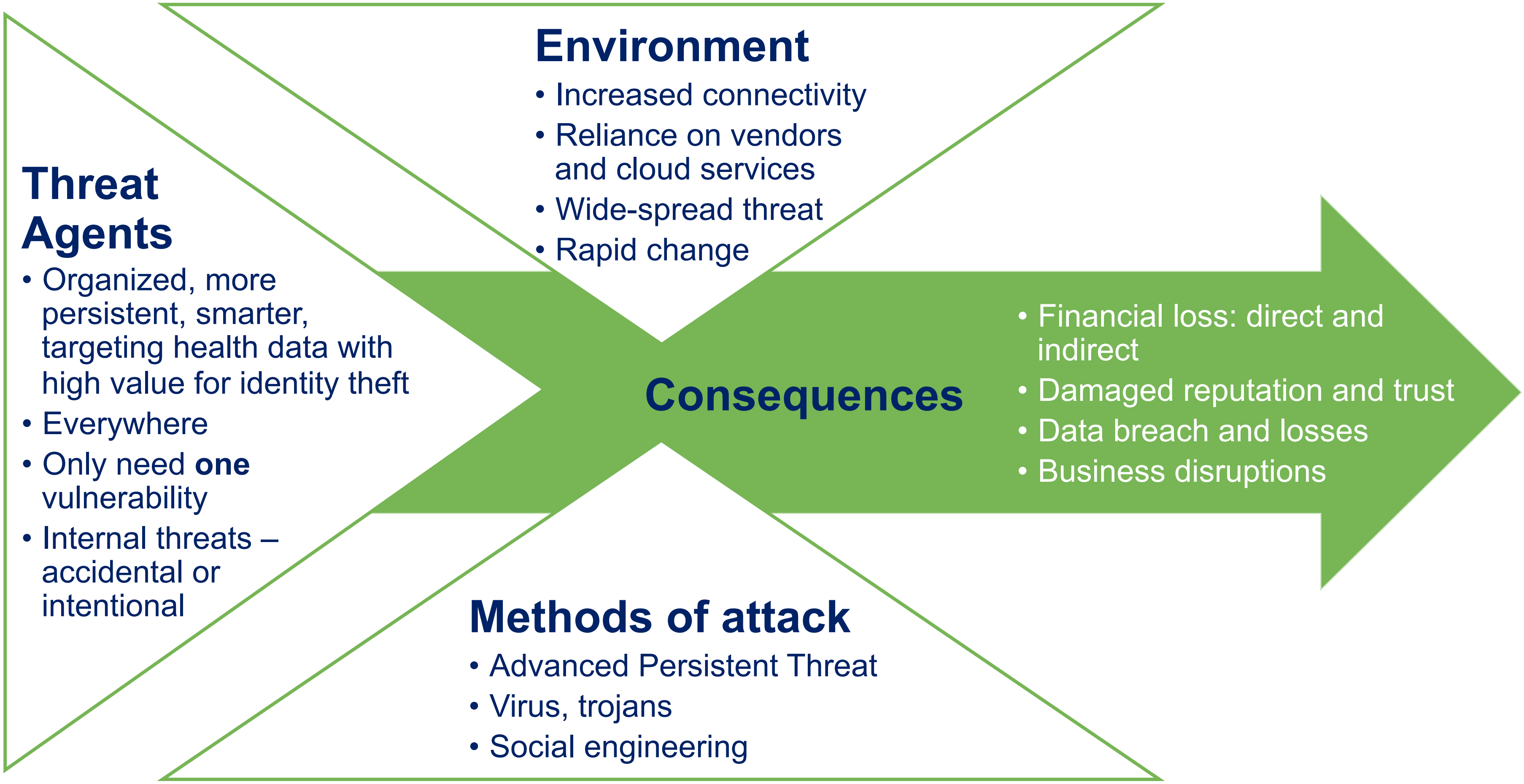
Defending against cyber security threats

Jesse Bowen, PhD, CISSP, CISM
Accenture Partner and Health Security Lead

July 2011

The cyber security ecosystem

Understanding the adversary, the environment and the methods of attack is necessary to create a sound cyber security strategy.



Threat Agents

- Organized, more persistent, smarter, targeting health data with high value for identity theft
- Everywhere
- Only need **one** vulnerability
- Internal threats – accidental or intentional

Environment

- Increased connectivity
- Reliance on vendors and cloud services
- Wide-spread threat
- Rapid change

Methods of attack

- Advanced Persistent Threat
- Virus, trojans
- Social engineering

Consequences

- Financial loss: direct and indirect
- Damaged reputation and trust
- Data breach and losses
- Business disruptions

Mobile devices bring new risks

- Devices have the capability to store much personal and often corporate information
- Wide variety of operating systems and hardware components
- Interoperable communication channels
- Always-on-and-synchronized nature
- Few have security controls implemented
- Often personally owned, affording less organizational control

Key principles of cyber security

1. Identify and secure IT assets themselves, not just the perimeter.
2. Build an effective “culture of security.”
3. Pay close attention to applications, vendor services, and partners.
4. Check and double-check user identity.
5. Develop acute situational awareness.

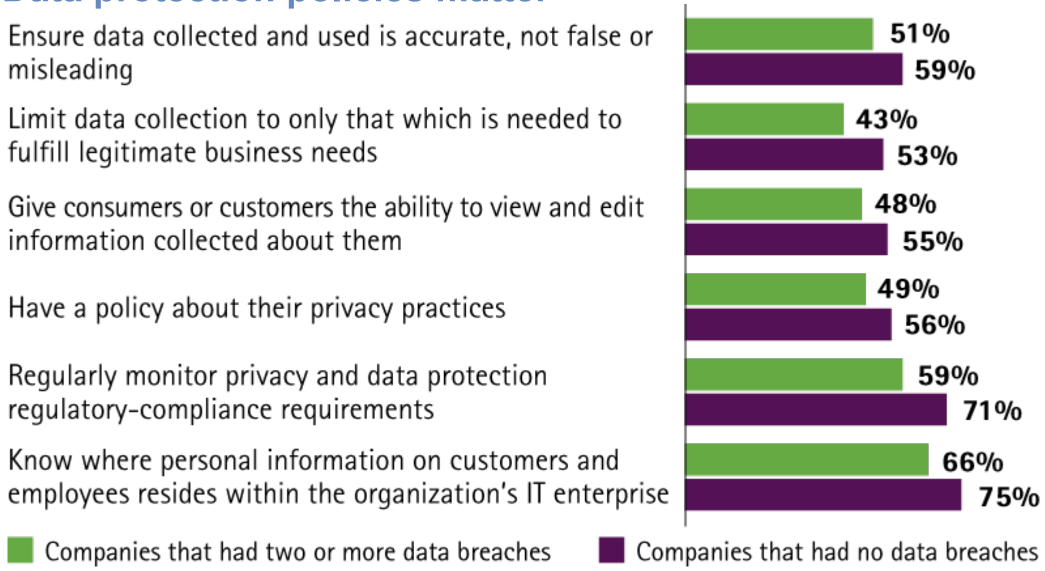
1. Identify and secure IT assets themselves, not just the perimeter

- Identify data and technology that are essential to operations and business continuity (many large organization have not yet done so).
- Create a detailed plan to protect these assets and capabilities, not just the perimeter.
- Assure plan meets regulatory, compliance, privacy and business demands.
- Assure plan viability with robust test.
- Embed cyber resilience and defensive capabilities throughout the organization, not just individual components.

2. Build an effective “culture of security”

- Clearly, explicitly define who is responsible for cyber security.
- Ensure a holistic approach to information management and protection.
- Consider your organization a steward, not an owner of personal data.
- Implement strong data protection policies.

Data protection policies matter*



*Source: Accenture survey, 2009.

3. Pay close attention to applications and vendor services

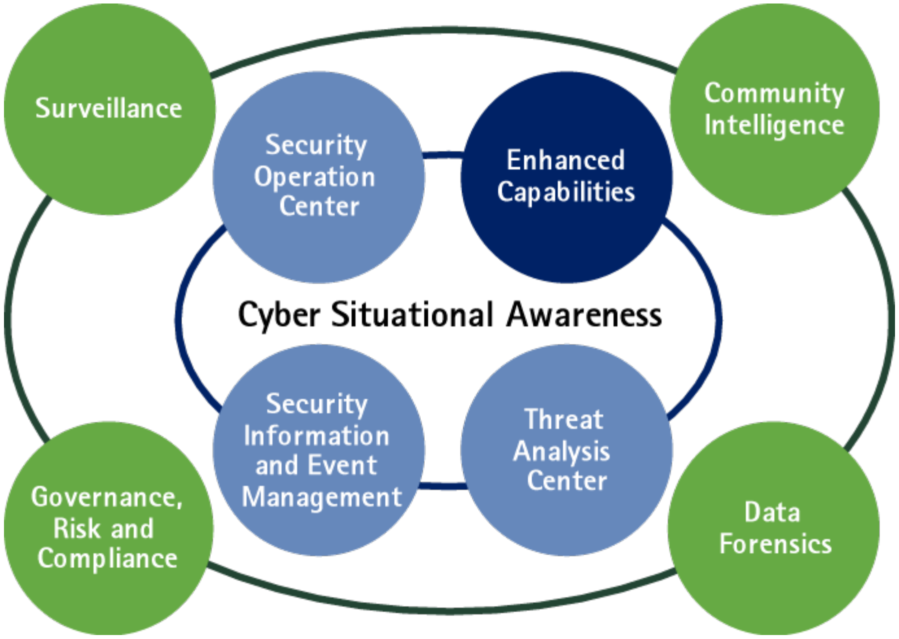
- Many serious breaches result from application-level weaknesses.
- Most developers have not included security in their applications, assuming the software would run inside a secure perimeter.
- Extend security to device level as well as to application layer.
- Assess security strength of off-the-shelf applications.
- Evaluate complete security architecture of service providers.

4. Check and double-check user identity

- Stop relying on authentication information (e.g. mother's maiden name) that has become more available or discoverable.
- Integrate strong authentication technologies with access management technologies.
- Biometrics (fingerprint, retinal scans), smart cards becoming more cost-effective.
- Embed pervasive security while maintaining ease of use (e.g. single sign-on, immediate access revocation, self-service functionality, real-time analysis).
- Consider two-factor authentication (e.g. smart card plus password).

5. Develop acute situational awareness

Situational awareness capability map


Surveillance
Security Operation Center
Enhanced Capabilities
Community Intelligence
Cyber Situational Awareness
Governance, Risk and Compliance
Security Information and Event Management
Threat Analysis Center
Data Forensics

- Attackers begin work long before detectable event.
- Organizations must:
  - Understand risk across entire landscape, including supply chain, business partners.
  - Recognize back doors and vulnerabilities.
  - Recognize complex and chained patterns that indicate attack initiation.
  - Expand scope of vulnerability assessment or penetration tests.
  - Harness external sources of threat intelligence.
  - Detect reconnaissance activity by a terminated employee or a hacker forum.

Appendix

> “Every year, an amount of intellectual property many times larger than all the intellectual property contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government agencies.”
>
> U.S. Sec. of Defense, William Lynn

The environment

- **Corporations operate in the cyber space.** Every aspect of the business depends on Internet-oriented computing and communications.
- **Security is not built in.** Systems that designers assumed would operate behind physical or logical barriers are now accessible via networks.
- **Change is constant.** A “good enough” defense today won't be good enough in six months.
- **Corporations are lucrative targets.** Attackers can gain intellectual property, personally identifiable information, sensitive competitive data, etc.
- **No one is immune.** Google reported losing intellectual property in a Dec. 2009 attack based in China. Cyber thieves stole more than $1 million in a July 2010 attack on 3,000 customers of a British bank.

  And the list goes on.

The adversary

Today's intruders rarely fit the image of a lone wolf probing corporate systems for bragging rights.

- Adversaries are smarter, better organized, more persistent. Many are part of criminal organizations, some are agents for nation-states.
- Attackers have a huge advantage. In cyber, offense is far cheaper and easier than defense, which must be 100% effective. The adversary needs only to find one weakness.
- Variety of adversaries and motivations leads to variety of attack types.

The methods of attack

Adversaries only need to find one vulnerability— and their methods of attack are multiple and rapidly changing

- Advanced Persistent Threats are targeted, “low and slow” attacks that stealthily move through a network without generating regular or predictable network traffic.
- U.S. military’s worst attack was launched from USB thumb drive bearing malicious program from foreign intelligence agency.
- Virus hidden on legitimate websites infected British bank customers’ computers, stole money from their online accounts.
- Google attack began with instant message sent to Google employee, who clicked a link to a poisoned website.
- Some attackers infect commercial software, hardware with “logic bombs” before it is sold.

Threats from within

Many of today's cyber security threats result from the behavior of organizations' employees.

- Using popular social networking Websites, possibly exposing employers' computers and networks to worms, malware, etc.
- Checking corporate email from unsecured personal devices, including smart phones and home computers.
- Self-provisioning potentially unsecure cloud-based applications.
- Accessing organization data from unsecure WIFI hotspots.

Security breaches have serious business consequences

Not just a technical issue

- In 2009, security breaches cost organizations an average of $6.6 million each—up from $6.3 million in 2007 and $4.7 million in 2006.*
- Stock prices of publicly-held companies typically drop five percent when breaches are made public.
- Fines and lawsuit losses can exceed $100 million.
- The loss of intellectual property due to cyber attacks can be significant.
- Cyber attacks can disrupt business operations (production interruptions, inability to process sales, etc.).
- Brand reputation and consumer and partner trust can be severely damaged by a data breach.

* Fourth Annual US Cost of Data Breach Study, 2009, Ponemon Institute