PROVIDENCE
Health & Services

What Will Tomorrow Bring?

Eric Cowperthwaite, CSO

ISSA CISO Forum – Houston, TX

February 29, 2008

Enterprise Security

"We meet at a college noted for knowledge, in a city noted for progress, in a State noted for strength, and we stand in need of all three, for we meet in an hour of change and challenge, in a decade of hope and fear, in an age of both knowledge and ignorance. The greater our knowledge increases, the greater our ignorance unfolds."

Address at Rice University on the Nation's Space Effort
President John F. Kennedy
Houston, Texas

September 12, 1962

Strategy

From Mintzberg: ”

1. Strategy is a plan, a "how," a means of getting from here to there.

2. Strategy is a pattern in actions over time; for example, a company that regularly markets very expensive products is using a "high end" strategy.

3. Strategy is position; that is, it reflects decisions to offer particular products or services in particular markets.

4. Strategy is perspective, that is, vision and direction."

Strategy

"A strategy is a plan to achieve a set of objectives where the plan represents the optimum balance between the competing demands of multiple stakeholders."

-Mintzberg

The Business Challenges

- The more things change …
  - Globalization
  - The Networked World
  - Asymmetrical conflict
  - The "millennial world"
- The more they stay the same …
  - Regulation
  - Market share and profit margin
 - Quality and leadership

Globalization

- **The human work force is more mobile than ever**
  - Telecommuting globally
  - Globally located "virtual teams"

- **Globalization is not just "bad"**
  - Tapping the resources of the entire world
  - A massive wealth expansion is taking place

- **New realities are emerging**
  - Jobs and markets are moving globally, not just regionally
  - The global revolution will mean disruptive change

The Networked World

- ## The "winners" will …

  – Communicate rapidly and effectively

  – Leverage the best resources globally

  – Deliver products to market "on the web"

  – Deliver on the promise we see in Web 2.0
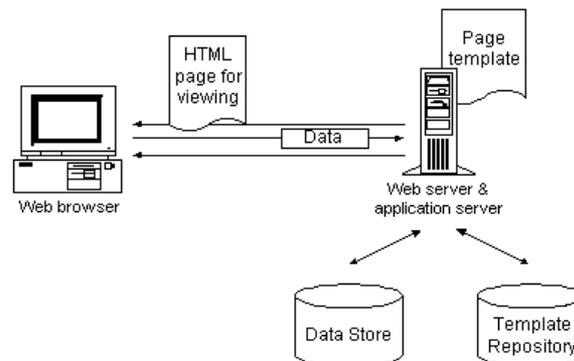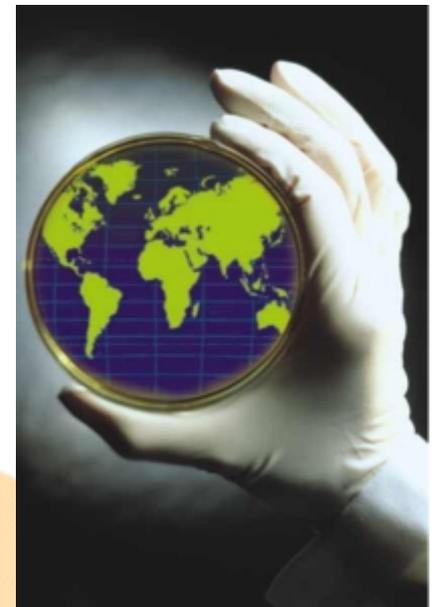
Asymmetrical Conflict

- **The "powers that be" are unassailable directly**

- **Rather than confront directly, the weaknesses will be sought out and attacked asymmetrically**

- **The Information Age equalizes an individual with an idea and a nation-state**

- **And it equalizes an individual with an idea and a Fortune 500 company**

The "Millenial Landscape"

- **More change will occur between 2009 and 2020 than in all of human history prior to today.**

    – By 2030 change will be so rapid and explosive that we cannot see beyond the "event horizon" and understand the changes

- **The "Digital Generation" begins to come of age in 2011**

    – Used to rapid, mass communication

    – Accustomed to internet based computing

- **Computing power will grow dramatically by 2020:**

    – In 2012 a laptop will be comparable to a cat's brain

    – In 2020 a laptop will be comparable to a human brain

The More They Stay The Same …

- **First World countries will regulate business more deeply**
  - SOX, HIPAA, FFIEC, SB1386, and ABC123
  - This will continue in mature markets

- **Competition for profit margin and markets will continue**
  - More competitors looking to capitalize on the wealth expansion
  - New markets emerging in Asia, Africa, South America

- **Quality products and services succeed**
  - The networked world makes poor quality transparent

- **Leadership will continue to be the critical success factor**

PROVIDENCE
Health & Services

The Security Challenges

- The more things change ...
  - New bad guys
  - More sophisticated malware
  - "Black Swan" events

- The more things stay the same …
  - Budget pressure
  - Tension between IT and security
  - End user desire for ease of use

The More Things Change …

- **Dramatically increased threats for information security**

- **Undisclosed Zero Day vulnerabilities**

    - Bad guys hire vulnerability researchers

- **New laws and regulations unforeseen today**

    - Remember SB1386 in 2003?

- **Consumer demands for increased security**

    - Protect identity data

- **"Black Swan" Events**

    - 9/11, Choicepoint, TJ Maxx, Virginia Tech

More About New Attacks

- **The PushDo Trojan**
  - Contains a software distribution system
  - Advanced tracking and hiding mechanisms
  - Geo coding and country white lists for specific geo targeting to "safe" locations
  - IP Address logging and tracking
  - Determines whether it is infecting a virtual or physical machine
  - http://www.eweek.com/c/a/Security/Inside-a-Modern-Malware-Distribution-System/

PROVIDENCE
Health & Services

More About The Bad Guys

- **We all know that they shifted from fame to profit**

- **Just how sophisticated are they?**

  – Clear, defined roles and responsibilities

  – Distribution channels

  – Distributors provide trojan and botnet services for pay

  – A fairly well developed "Malware Economy" now exists

  – The Malware Ecosystem is modeled after Software VAR ecosystems

More About Black Swan Events

Probability

High Probability / Low Impact **"Low hanging Fruit"** **e.g. virus, port scans**	**High Probability / High Impact** **The "Must Do" Risks** **e.g. identity data loss**
Low Probability / Low Impact **Easy to Address** **e.g. internal spam**	**Low Probability / High Impact** **The "Black Swan" Events** **e.g. Mt. Rainer, 9/11**
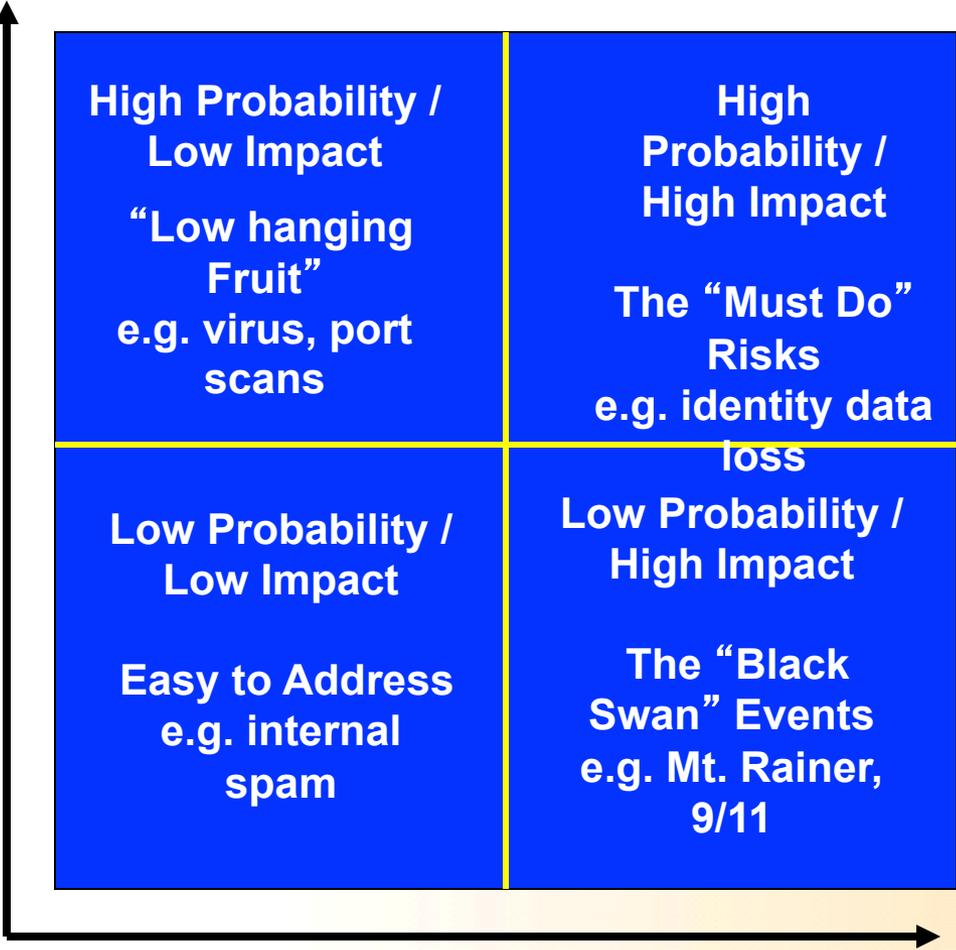
Impact

These risks and events are the ones that change how we do things and the world we live in.
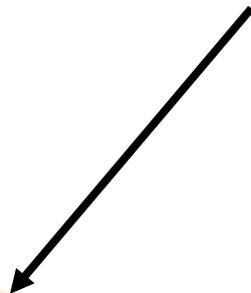
Expanding Upon "Black Swan" Events

- **Most risks are predictable and can be mitigated**

  – High Impact, Low Likelihood risks are outliers

- **Black Swan events are generated by these risks**

- **They *will* occur and they *will* catch us by surprise**

  – ChoicePoint, Providence Health & Services, TJ Maxx

  – In hindsight, they were predictable

  – All 3 cases were a perfect storm of under investment, over confidence, and a lack of understanding of the changed threat environment

- **All is not lost**

  – Solid planning, sound operations capabilities and preparing for the unknown

The More They Stay The Same

- **We will continue to tackle traditional issues**

  – Pressures on efficiency and budgets

  – The need for transparency

  – Traditional threats and vulnerabilities

  – Tension between IT operations and Security

  – Alignment with the business

  – Stakeholder desire for simplicity and ease of use

Aligning Security With The Business

- Security is a business function, and so you must …

  – Achieve (or even create) a common perspective for both business and security leaders

  – Focus on the key business drivers.

  – Contribute to the success of the business

A Common Perspective

- **Security as a cost of doing business**
    - Determine what functions are part of due diligence and good business practices
    - Build a set of due diligence security controls that are a minimum standard
    - The core function of security is to protect employees, customers, information and assets

Security as a business value add
    - Determine how security can reduce cost, increase efficiency and align with business strategy
    - Security projects and capital spend must bring value to the business.

- **Security as a risk management tool**
    - Now, what risk remains, and how can we reduce it?
    - Risk is unrealized operational expense

Security's Core Business Function

- **Security is a business function and it must:**

  - Protect employees, customers, information and assets

  - Drive operational costs down, year over year

  - Be measurable in meaningful terms

  - Contribute to increased competitiveness and profitability

  - Align with the strategic direction and plans of the business

What Does That Mean?

- The foundation of security is operations, not risk

- Operations must improve efficiency and productivity year over year

- Investment is critical to aligning with the business, not risk

- Risk is how we identify where to invest tomorrow

So That We Can Deliver

- Enhanced profitability

    – Drive down overhead and operating cost

    – Improve efficiency and productivity

    – Reduce unrealized expense (i.e. security risk)

- A clear differentiator for our business

- And, the bottom line:

    We appropriately protect the customers, employees, information and assets of our business

Security Success in 2009 and Beyond

- **Security must be ….**

  - Process based with predictable outcomes

  - Service oriented

  - Flexible and agile

  - Intelligent

  - Prepared for the unknown

And So ……….

To succeed in this landscape and do all the neat things …

It will require:

- Smart, agile people

- Participative planning and decision making

- Business Engagement

How The Heck Do I Do That?

- **Have smart, agile people**
  - **Hire quality, not quantity**
  - **Educate and train**
  - **Be compassionately ruthless**

- **Participative planning and decision making**
  - **Your team**
  - **Your stakeholders**
  - **Your leaders**

- **Business Engagement**
  - **Regular meetings with senior execs and peers**
  - **Interact with the middle managers in the business**
  - **Create security managers/liasons for the business units**

At The End Of The Day

- **To succeed, you must ….**

  – **Understand the challenges of the business**

  – **Prepare for the security challenges you will face**

  – **Align security to support success**

  – **Support your organization's strategy**

Suggested Reading

- "The Black Swan: The Impact of the Highly Improbable", Nassim Nicholas Taleb

- "Wikinomics : How Mass Collaboration Changes Everything", Don Tapscott

- "Freakonomics : A Rogue Economist Explores the Hidden Side of Everything", Steven D. Levitt

- "The Singularity Is Near: When Humans Transcend Biology", Ray Kurzweil