

Adapting To The New IT Security Realities

Jonathan Penn, Vice President
Forrester Research

February, 2011

FORRESTER®

Unprecedented industry change

Business And IT Disruption

**New industry
economics**

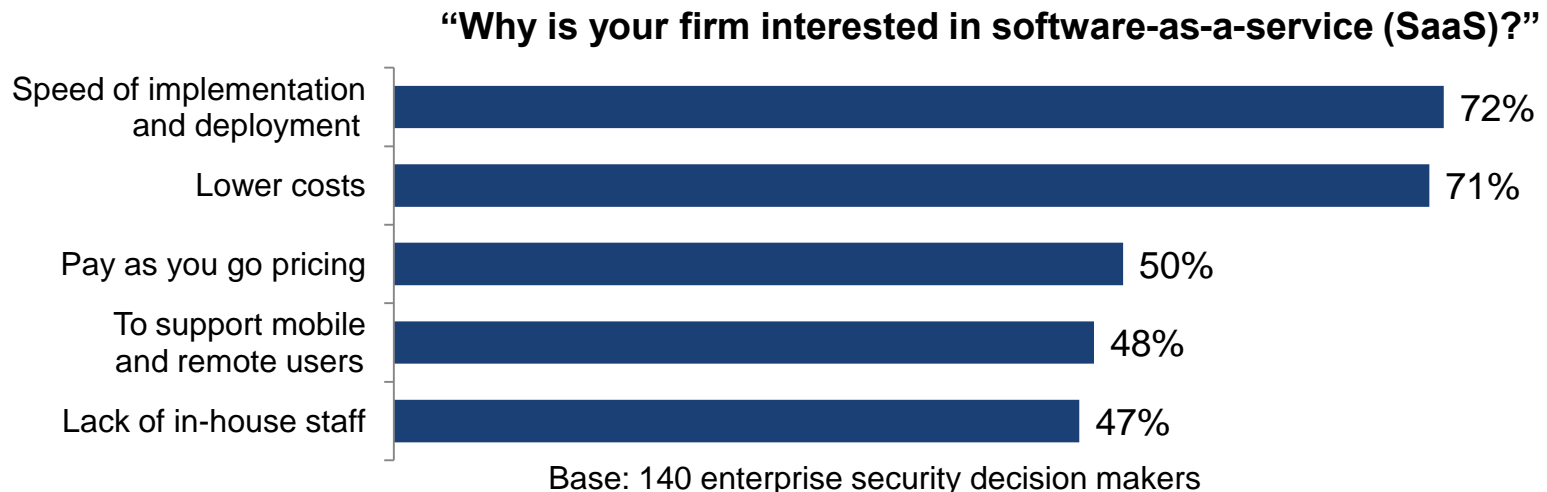
**Shifts in
decision making**

**Technology
revolutions**

New industry economics

Services-led IT investments will become the norm

- The restructuring economy accelerates **adoption of “as-a-Service”**
 - Better TCO: per-use pricing, OpEx vs. CapEx, faster deployment/upgrade cycles
- Growing need for **external domain expertise**
 - Technical complexity and pace of technology change
 - Ongoing staffing and budget pressures



New industry economics

Services-led IT investments will become the norm

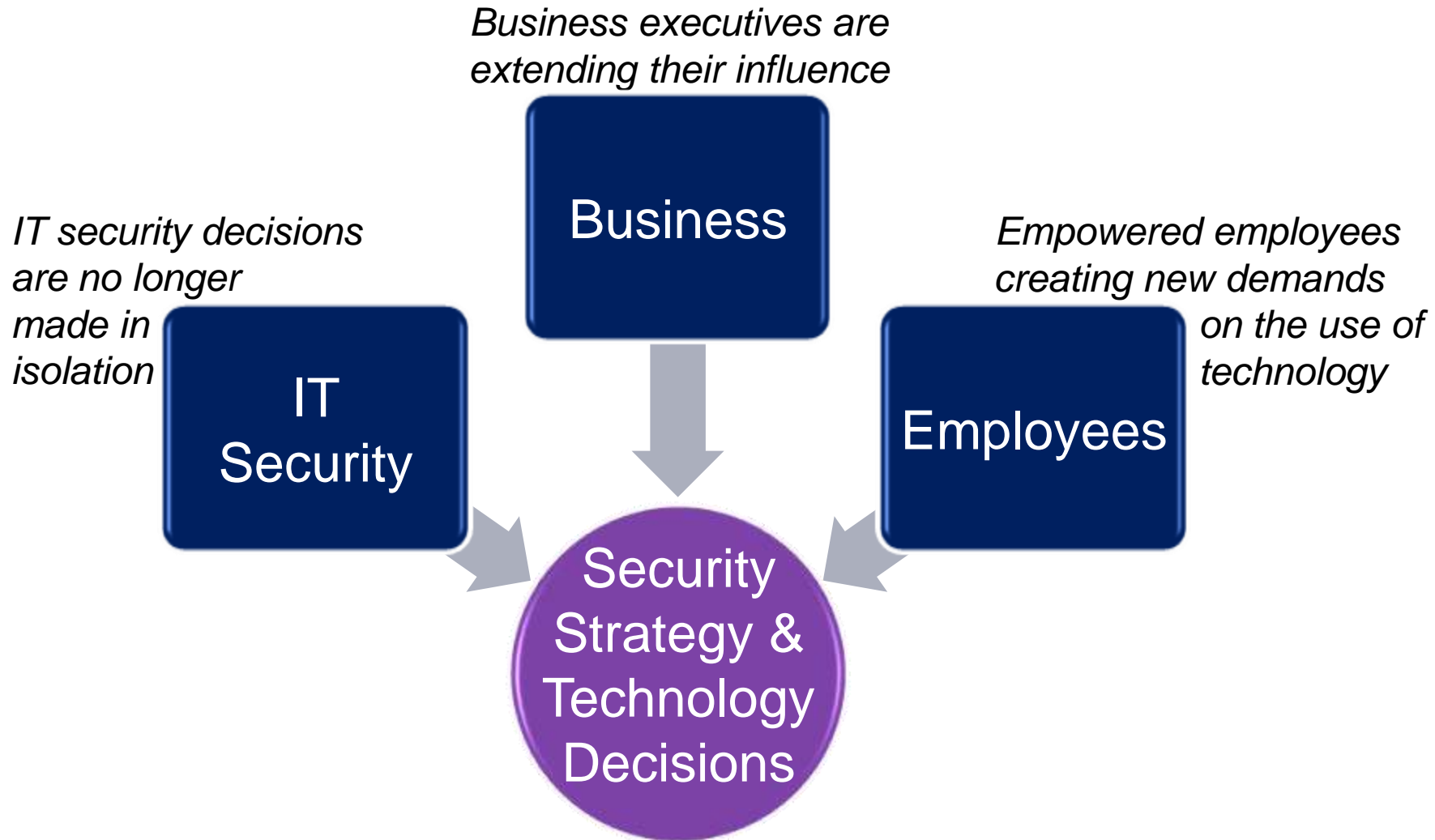
- The restructuring economy accelerates **adoption of “as-a-Service”**
 - Better TCO: per-use pricing, OpEx vs. CapEx, faster deployment/upgrade cycles
- Growing need for **external domain expertise**
 - Technical complexity and pace of technology change
 - Ongoing staffing and budget pressures

“How important were the following in driving your firm’s adoption of managed or SaaS security services?”



Base: 715 enterprise security decision makers

Shifts in decision making





Virtualization

Cloud & SaaS

Technology Revolutions

Web 2.0

**Mobility /
Device Diversity**



And of course...the threat landscape



Motivation

**From fame to financial gain
(Zeus)**

Method

**From audacious to “low and slow”
(Aurora)**



Focus

**From indiscriminate to targeted
(Stuxnet)**

Impact

**From disruptive to disastrous
(WikiLeaks)**



Cheer up...

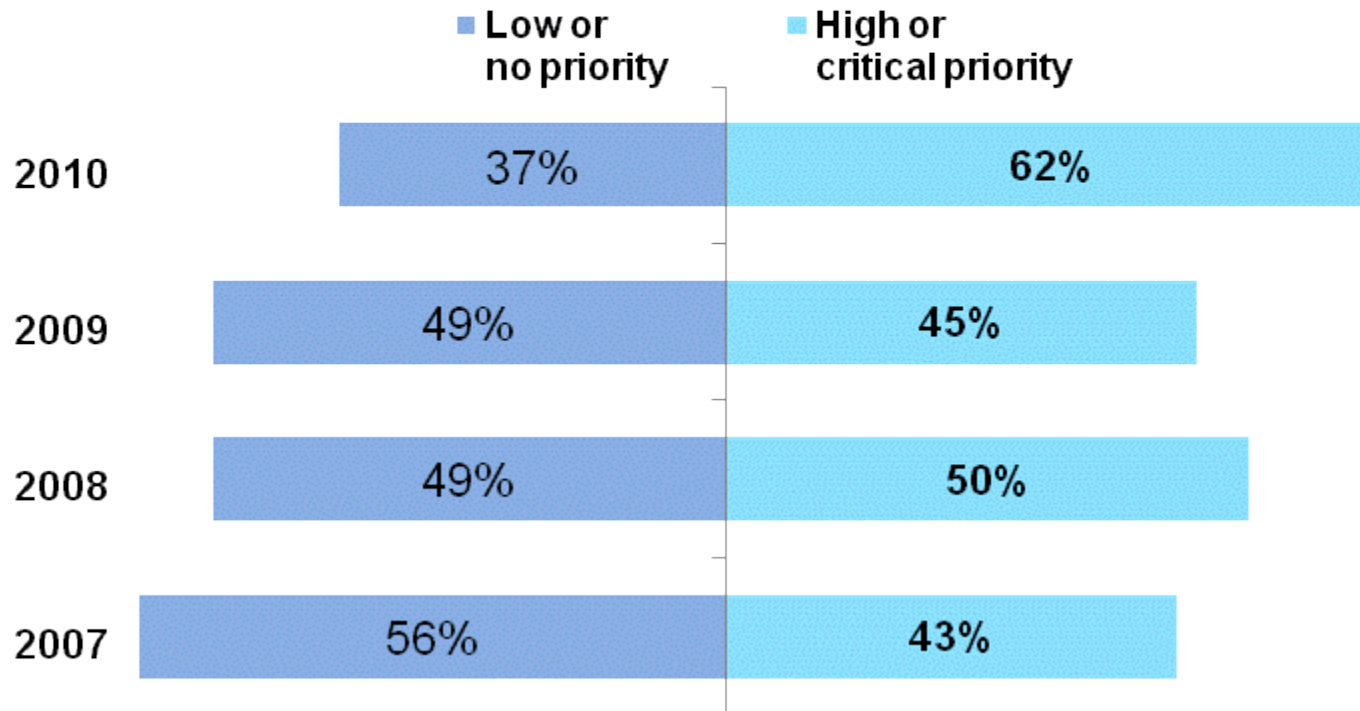


**...it's not
as bad as
it seems.**

Security is more a priority than ever

“Which of the following initiatives are likely to be your IT organization’s top technical priorities over the next 12 months?”

Significantly upgrade our security environment



Base: 2,803 North American and European IT budget and priority decision-makers

Source: Forrester Global IT Budgets, Priorities, And Emerging Technology Tracking Survey, Q2 2010

IT security struggles to deliver capabilities matching their growing responsibilities and business' expectations

- It's no longer just about managing firewalls and AV
 - Monitoring the environment and preventing intrusions
 - Achieving and maintaining compliance (regulatory, internal, 3rd party)
 - Ensuring business continuity
 - Measuring and managing IT risk

“Please rate the following IT security challenges in your firm.”



Base: 2,058 North American and European IT security decision-makers

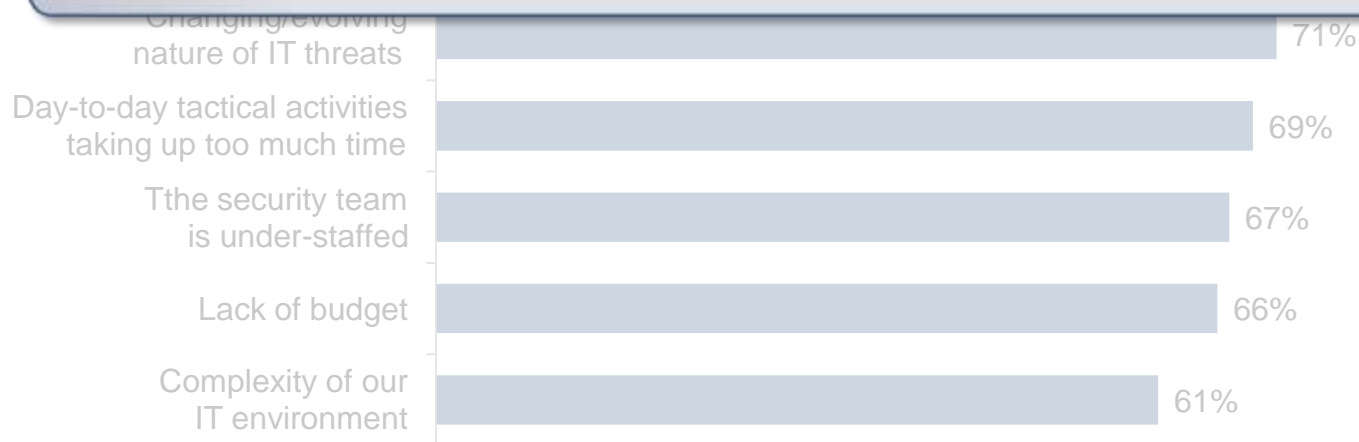
Source: Forrester Forrsights™ Security Survey, Q3 2010



IT security struggles to deliver capabilities matching their growing responsibilities and business' expectations

- It's no longer just about managing firewalls and AV
 - Monitoring the environment and preventing intrusions
 - Achieving and maintaining compliance (regulatory, internal, 3rd party)
 - Ensuring business continuity
 - Measuring and managing IT risk

“There are an overwhelming number of things we need to do for security, but I simply don't have the resources. Projects we want done in the next 6-12 months are instead 3-5 years out in our planning.” (IT executive at a large healthcare provider)



Base: 2,058 North American and European IT security decision-makers

Source: Forrester Forrsights™ Security Survey, Q3 2010



Build on reactive controls with preventive ones

Examples

- 1. Insurance firm wanting to identify everywhere it was storing personal information of its customers**
 - Used eDiscovery tool to find hundreds of places where PII was being stored without proper controls. Centralized this data, and put encryption and tighter access controls in place.
- 2. Retailer seeking to comply with PCI DSS**
 - Created corporate encryption standards for newly deployed applications. For legacy applications processing cardholder data, it created a network enclave for servers, deploying tape encryption for backups going offsite.
- 3. Large bank combating fraud**
 - Subscribe to SaaS-based fraud detection solutions that analyzes activity across its customer base to identify malicious or compromised PCs and accounts, suspicious users, and changing attack tactics

Operationalize or outsource tactical activities

Examples

- 1. Professional services firm streamlining security operations lifecycle**
 - Had the same people manage client security, client management, and network access control. Built a process to identify problems, enforce the right access privilege, and remediate any non-compliance deficits through one point-and-click console.
- 2. Bank overwhelmed with security information but not enough insight**
 - Outsourced the repetitive elements of security monitoring to an MSSP with the operational and analytical expertise, retaining in-house the functions related to business impact analysis.
- 3. International beverage company sought protection from vulnerabilities and help satisfying compliance requirements**
 - Contracted with an MSSP for comprehensive vulnerability scanning, around-the-clock intrusion prevention, and compliance reporting.

Focus on employee training to strengthen weak links

Training and awareness ties into overall security posture:

- A majority of breaches occur because of people inside your firewall¹
- Your personnel are your first and last lines of defense
- Training should educate employees as to:
 - Vigilance in their surroundings and identifying suspicious activity
 - Their responsibility for reporting security incidents
 - Where/how to report security incidents or suspicious activity
 - The common inadvertent activities that carry risk
 - Keeping evidence forensically 'clean'
- Training should be tailored to an employee's specific role, access, risks

¹ Source: Verizon Data Breach Report, 2010

Focus on communication and engagement with the business through formal and informal processes

Examples

1. Follow the money: build ties with key stakeholders

- The new CISO at an international manufacturing company started her tenure by quickly establishing a strong working relationship with the CFO, who held budget authority over the security group.

2. Weave security into business and IT decision-making

- Energy company established a governance and compliance function across the whole company for all IT systems, integrated into all the processes for strategy and costing, ensuring sound risk management.
- IT Security Director at a government agency developed a formal business liaison role to have staff sit with the business to understand their day-to-day issues and concerns.

3. Show value: up-level your security metrics

- CISO at a multinational conglomerate collects dozens of operational metrics, but reports to executives on just two: *loss* and *downtime*.

Leverage standards and formalized models to support your decision-making

Pain points

“Our IT security budgeting process is not scientific. We don’t say, ‘Based on this new problem, we’ll spend these additional dollars.’ I wish it were scientific, but we don’t have the data to support it.” (*Security Director, telecom company*)

Best practices

1. Use frameworks to organize the program and build credibility.

- Global bank embraces various frameworks (CoBIT, ISO, ITIL). This keeps their program well-organized and up to date. This builds credibility with executives, internal audit, and regulators that the program is comprehensive, up-to-date, and that gaps are identified.

2. Employ formal processes and tools to measure and manage IT risks.

- Government agency defined a methodology to identify risks and assess their controls and gaps: primarily data-value driven, but also taking some financial and operational risk into account.

Adopt new models for information security architecture

Examples

- 1. Manufacturer sought an efficient way to work with thousands of suppliers whose contract might only last a year or two.**
 - Now treats these applications – which also need to be widely accessible to internal resources – as Internet-accessible systems on its internal network, opening up the perimeter to more transparent access.
- 2. Retailer going through a reorganization wanted better enforcement of “least privilege” principles.**
 - Used DRM system to protect sensitive information like HR data, customer, and sales data. Greatly reduced the risk of a disgruntled employee misusing data, and also demonstrated due care to auditors.
- 3. Global telco redesigned network with more security chokepoints.**
 - All traffic now goes through a set of internal firewalls before hitting the network distribution layer, enabling more granular policy enforcement.

Thank you

Jonathan Penn

jpenn@forrester.com

www.forrester.com

