High performance. Delivered.

government of the future centre

Intelligent Security – Defending the Digital Enterprise

11th Aug, 2014

High level overview

Public Sector: Cyber Security and Public Sector – Why today?

Today: Key Business Challenges

A New Tomorrow: Approach to Intelligent Security

How to Get There? Security Call to Action

Cyber Security and Public Sector – Why today?

Headlines from Security Breaches

The Cybercrime Economy

Russian criminals steal 1.2 billion passwords

By James O'Toole and Jose Pagliery, @CNNTech August 6, 2014: 6:56 AM ET

NEW YORK (CNNMoney)

Russian criminals have stolen 1.2 billion Internet user names and passwords, amassing what could be the largest collection of stolen digital credentials in history, a respected security firm said Tuesday.

Since 2005:

148,398,723 Records Stolen
686 Breaches made public in Government Sector

Source: privacyrights.org
https://www.privacyrights.org/data-breach/new

Average Total Organizational Cost of Data Breach in US:
$ 5,403,600
Source: Ponemon Institute Report – May 2013

Why Public Sector? Why is security different for Public Sector today?

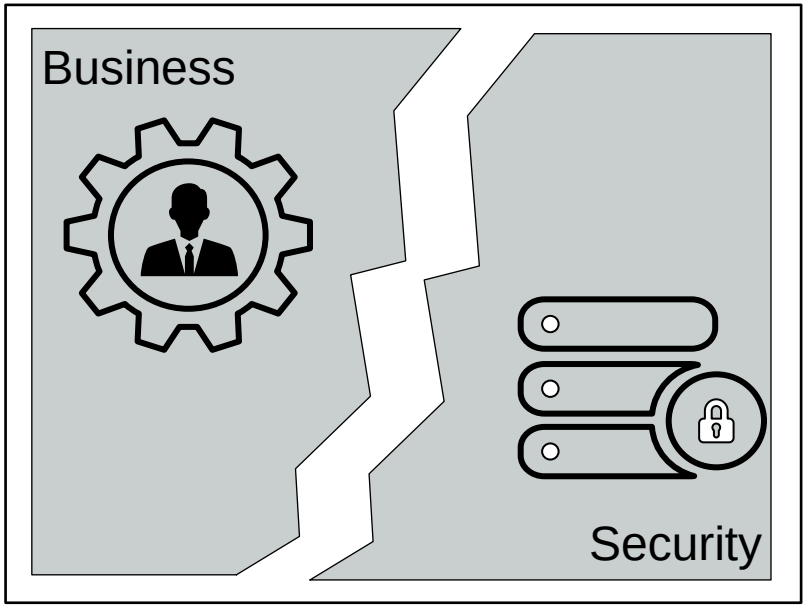
Real Attraction: *Citizen Data and Sensitive Information (Personal Data, SSN, DOB, Drivers License Health Records, Tax Records and so on).. And drive for E-enablement of Public Services with aging Infrastructure and funding constraints*

Change in threat landscape	• Threats in other channels are very different and can come from a variety of sources (e-Government, Cloud, Mobility etc.)
Under investment	• Public Sector is generally under-invested and under-prepared to manage threats coming from new channels
Easy Targets	• Risk appetite for Public Sector is generally high, along with under investment, making them easy targets
Change of regulations	• IRS, HIPAA, Privacy laws have been getting more stringent with every iteration.
Change in Corporate Accountability	• CIOs, CEOs etc. are getting fired rather than low level IT guys. Governors are watching this closely
No one wants to be the next Breached	• Brand & Reputation impact, loss of citizen trust, unwanted media attention

Today: Key Business Challenges

1. Missing the link between organization mission and security

Protecting the organization should be the first and foremost goal of any security program, but most enterprises do not make it a core competency

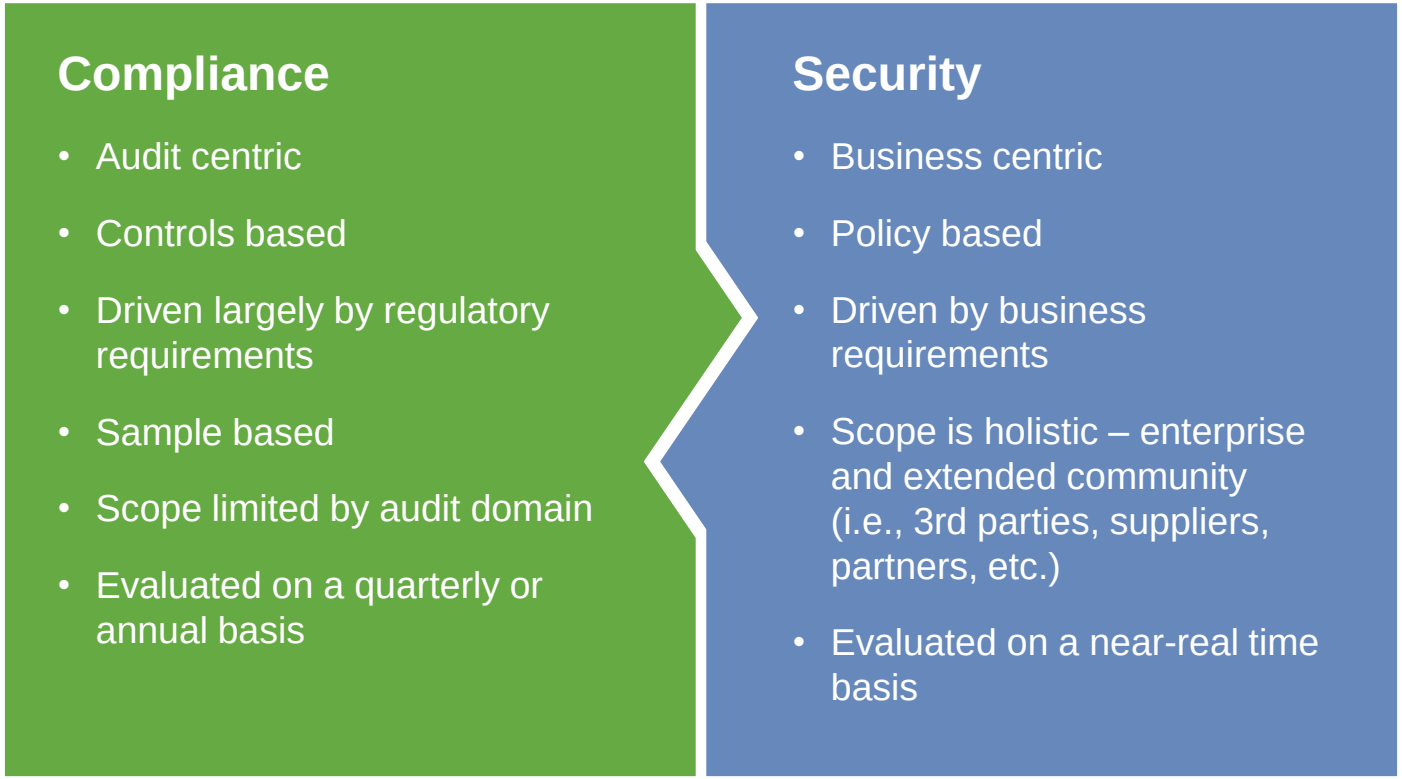


- Untethered programs can drift and become largely ineffective
- Some security executives might struggle to draw a clear line between the protection provided and its impact on the citizen satisfaction, loyalty and revenue
- The Security team may lack a logical road map for changing the organization's view of the security function as simply an inhibitor or cost center

Organizations need to tie their security programs to organization's mission and imperatives and actively engage key stakeholders in the security conversation

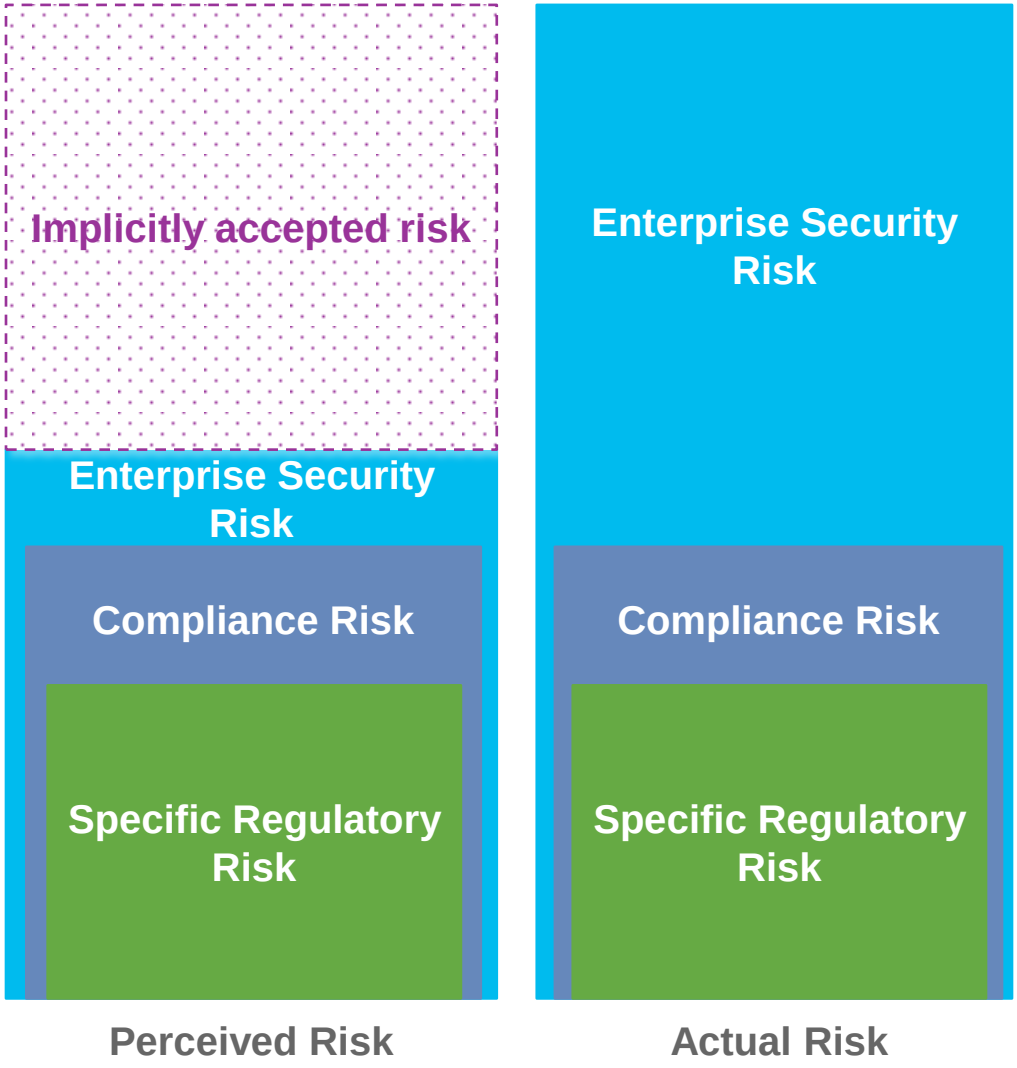
2. Thinking outside the compliance (check) box

Unfortunately, compliance does not ensure security. Instead, enterprises should view compliance as the minimum acceptable cyber security “bar” they need to clear…



Net result…

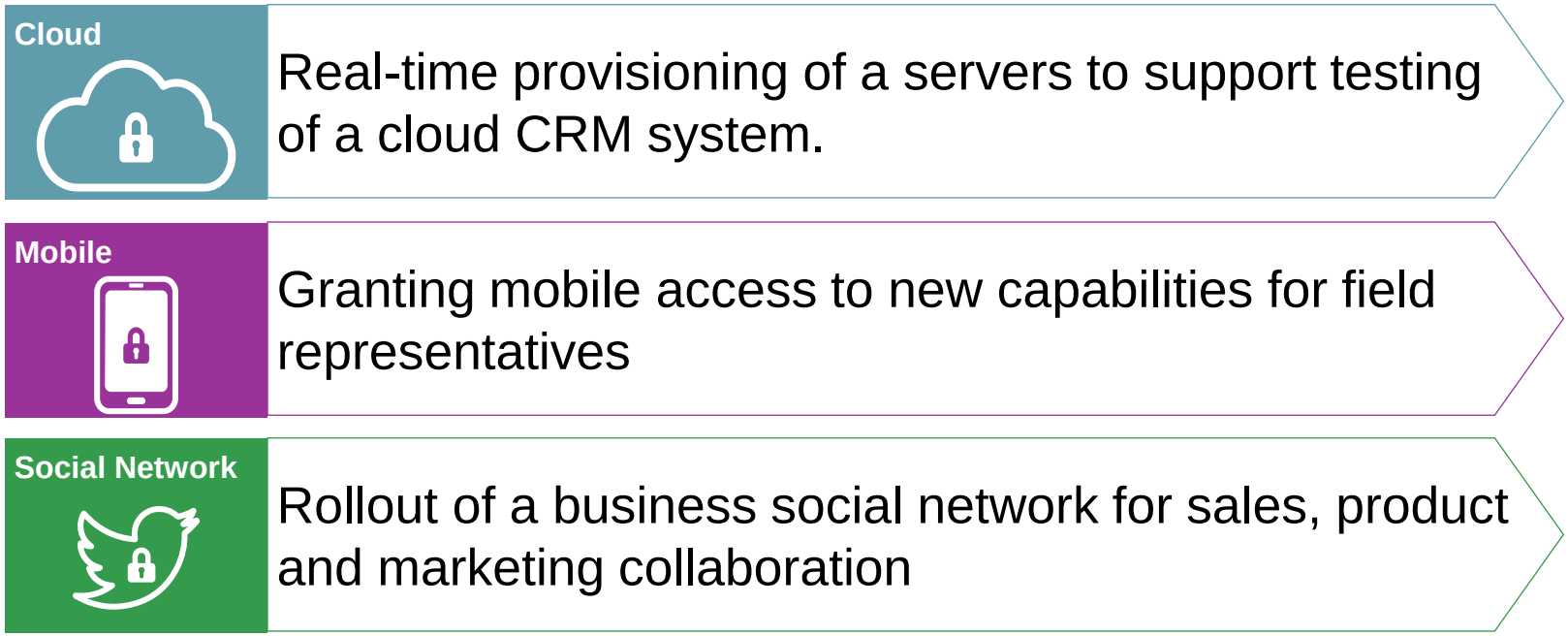
Compliance driven (or audit scope driven) security scope can cause organizations to implicitly and unknowingly accept a significant amount of cybersecurity risk



3. Governing the extended enterprise despite blurring boundaries

While business adoption has been widespread and rapid, many security organizations struggle to establish the appropriate frameworks, policies and controls to protect the expansions and contractions now common in extended IT environments

Typical Day in the Extended Enterprise



4. Keeping pace with persistent threats

As the threats become more persistent, they become harder to identify

Most organizations focus on:

- Monitoring – Difficulty in prioritizing critical events and handling uncertainty
- Static controls – Standard controls don't help once the attacker is in

For which cyber-threat are you prepared?

Opportunistic Acts

Attacker profile:

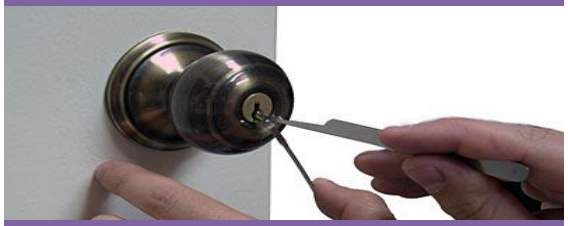
- Will move on if thwarted
- Will make mistakes
- Can be creative

Mob

Attacker profile:

- Emotional and not disciplined
- Not after the crown jewels
- Not well backed

Determined Actors

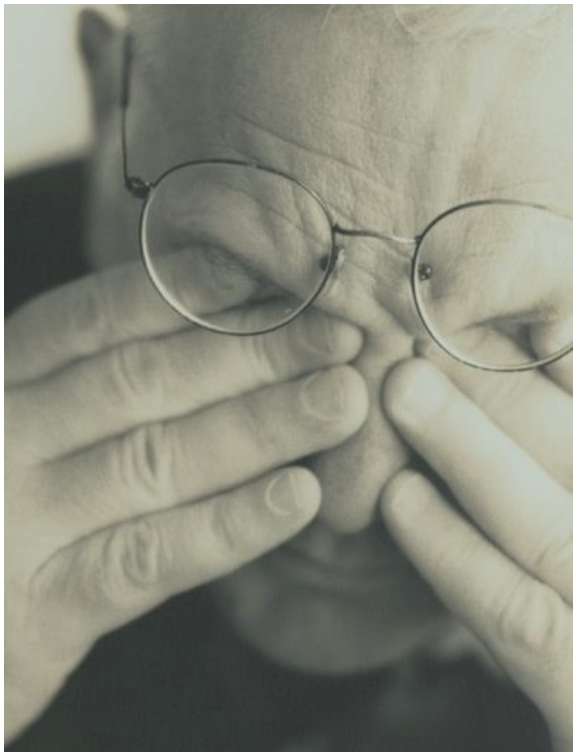


Attacker profile:

- Failure is not an option
- Need only one vulnerability
- Stick with it mentality

5. Addressing the security supply/demand imbalance

Most organizations lack sufficient security talent to address their current needs

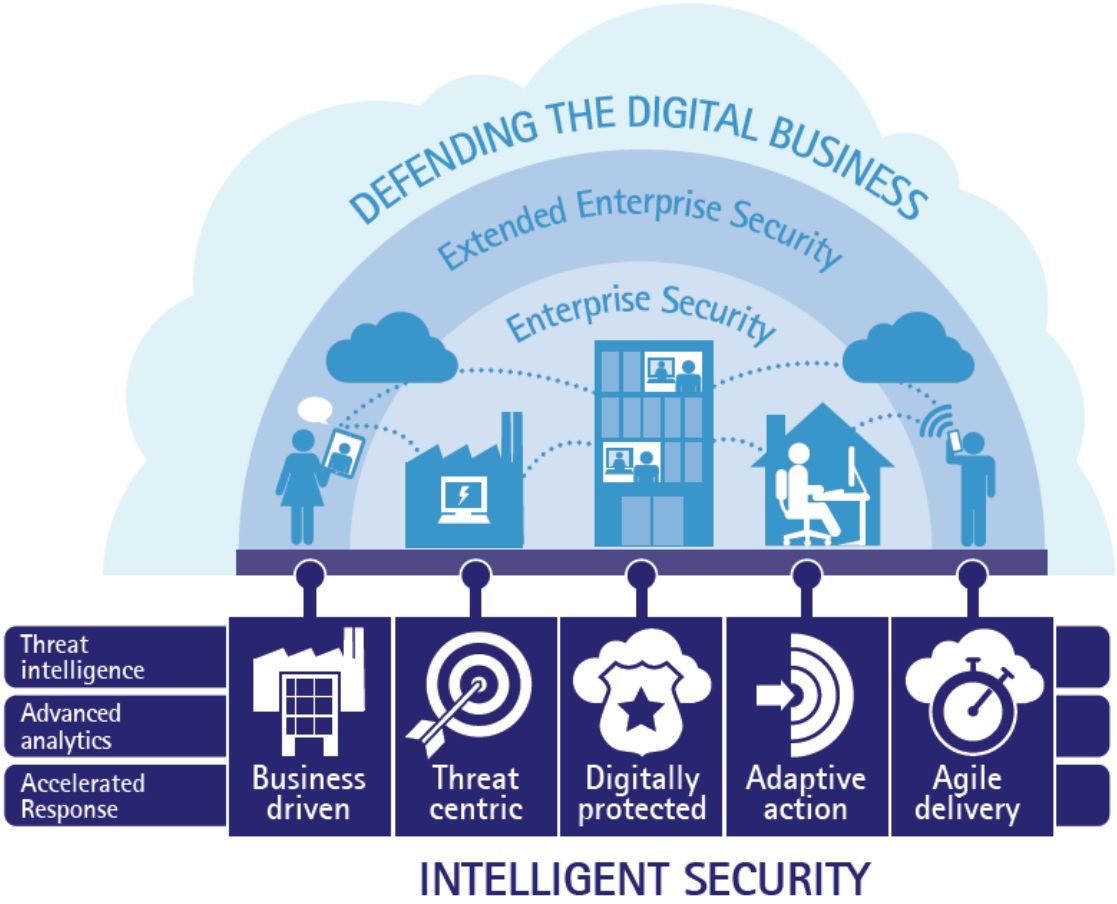


- **Skill Shortages**
  - Lack of the appropriate skills to execute required tasks
  - Hiring premiums for cyber security resources
- **Career Development**
  - Skilled resources are eager to keep skills sharp and maintain exposure to new technologies
- **Firefighting**
  - Misalignment of security programs to strategic business objectives cause practitioners to burn-out from constant troubleshooting

Defending the Digital Public Sector

Vision for Intelligent Security

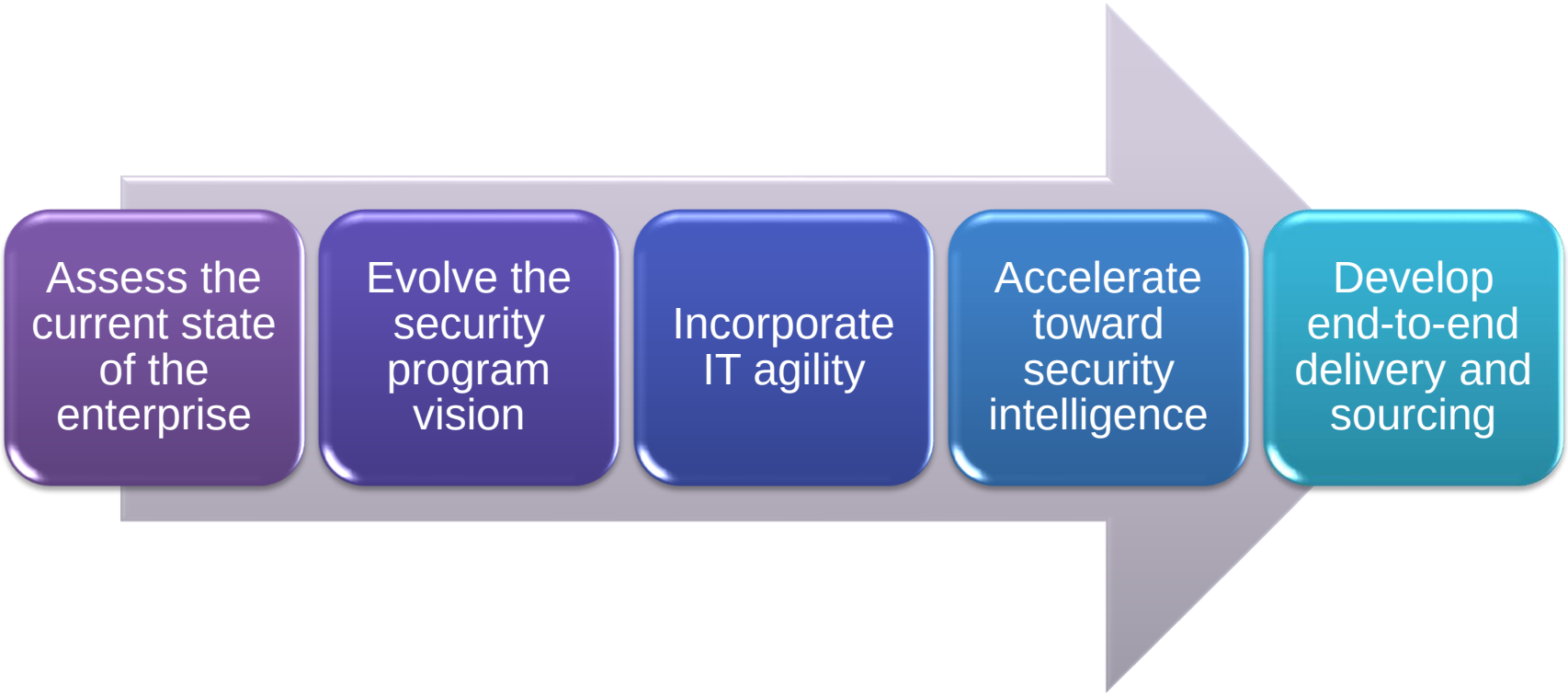
As organizations shift from a compliance-centered security mindset to an active cyber security stance, security teams need to adapt to keep pace with evolving business objectives



- ✓ Driven by a comprehensive security strategy that is aligned to business goals and objectives
- ✓ Core business assets protected by robust enterprise security controls
- ✓ Layered on top are extended enterprise safeguards focused on protecting cloud, mobile and social network vulnerabilities
- ✓ Security analytics and threat intelligence deliver cyber security intelligence to an orchestration layer for a swift, proactive and effective response
- ✓ Security metrics to measure enablement of business outcomes

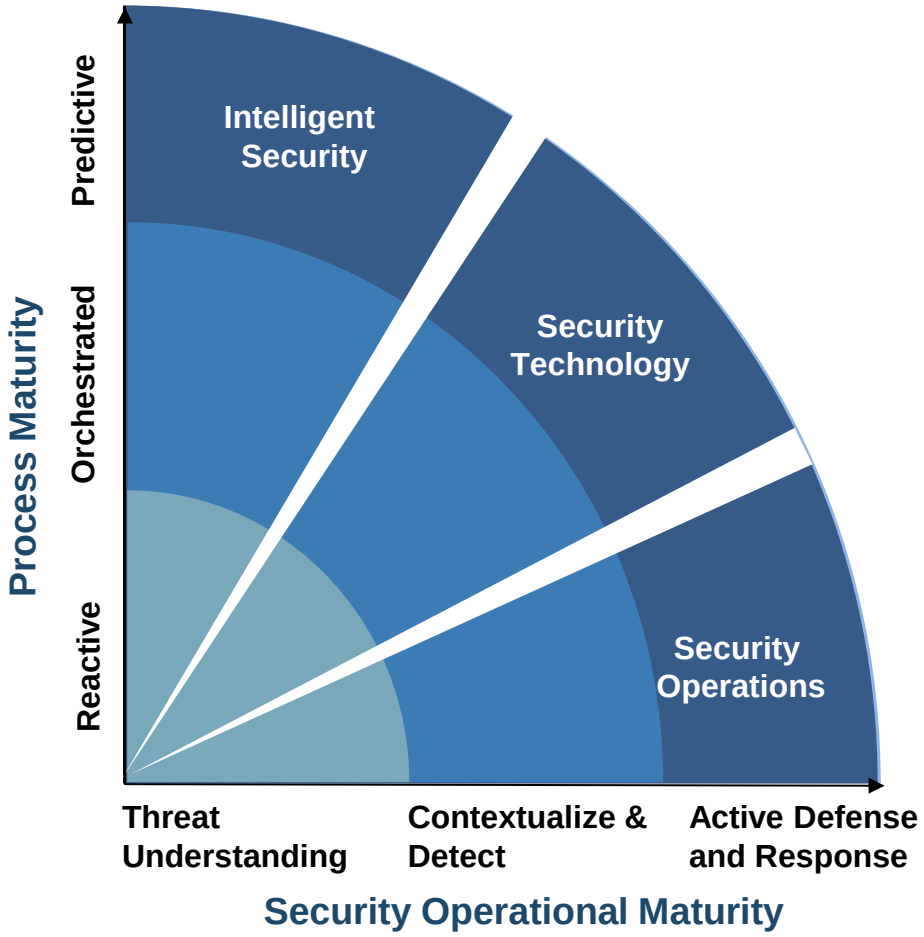
Taking the next steps to address Intelligent Security for the digital enterprise

Leading companies develop effective cyber security measures to handle vulnerabilities and mount an active defense calculated to meet and deflect attacker advances



1. Assess the security program's capability and identify leap-ahead opportunities

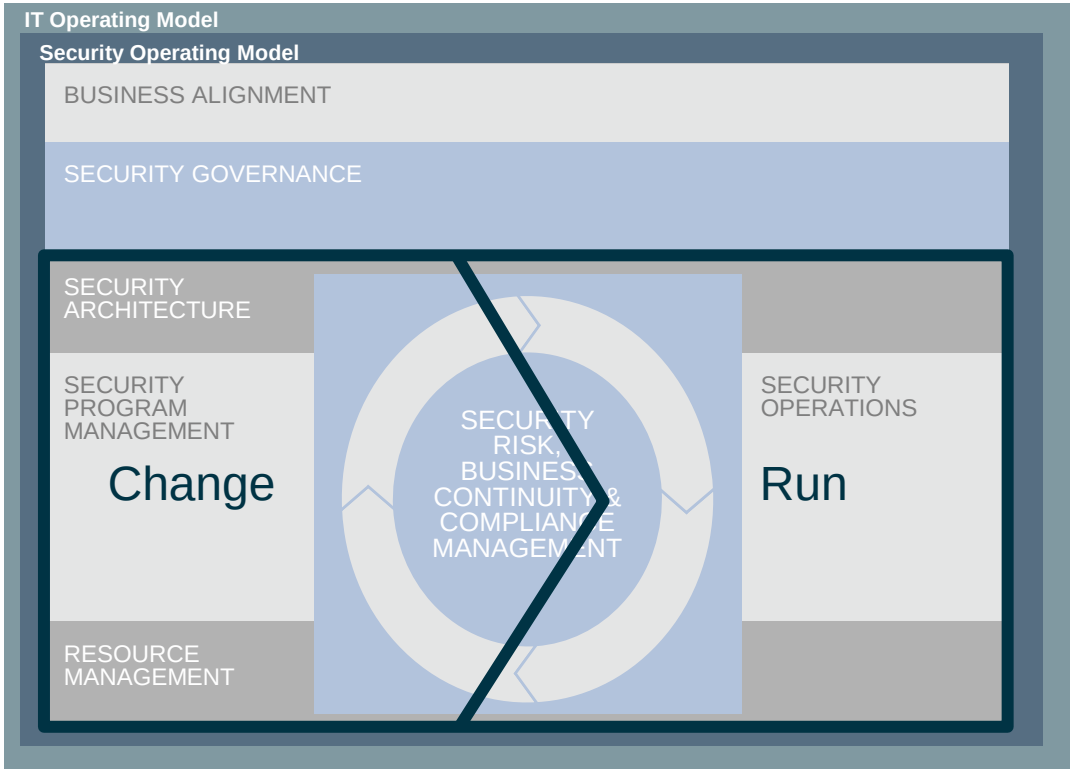
Before leaders can adopt a business-centered cyber security stance, they need to determine where their organizations currently stand and the level of resources required to support meaningful transformation



2. Manage complexity and integrate the enterprise

Establish an end-to-end enterprise security program and integrate it with existing enterprise architecture processes to reduce complexity levels and produce outcomes valued by the business

High-level view of Security Operating Model components



- Establish a new vision of how security integrates and works with IT and the business, effectively creating a security operating model
- Establish basic security operation across multiple organizational functions (roles, processes, metrics and governance policies)
- Develop a security technology process model and form the basis for security investment based on business attributes
- Integrate into the overall enterprise architecture, technology and processes

3. Become Agile

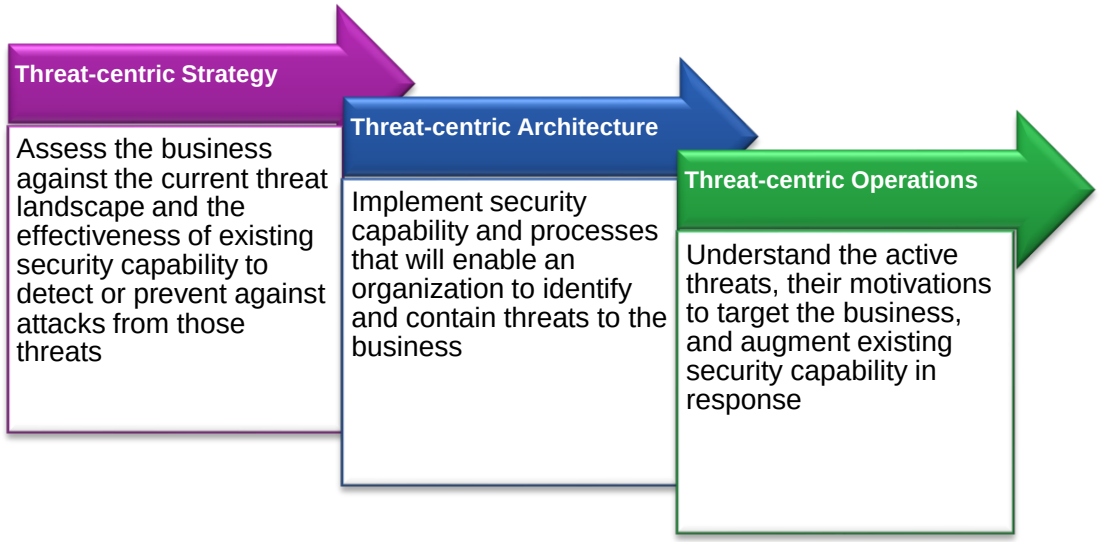
Embrace the cloud and other emerging technologies to boost IT agility and reach customers faster, capitalize on efficiency and cost benefits and do so within risk tolerances

Leaders achieve equal or better security posture by employing integrated security capabilities across their cloud, mobile and social networks. Organizations can take three key steps to make this approach work:

1. Consistently apply technical controls for and from the cloud to the extended enterprise
2. Craft contractual arrangements to address third-party service provider risk
3. Share responsibilities with cloud, mobile and social providers to improve agility in security operations.

When Threat is top of mind an organization…

- … drives strategy based on how they may be attacked
- … seeks to understand the shifting threat landscape
- … adapts to pre-empt threats targeting the business



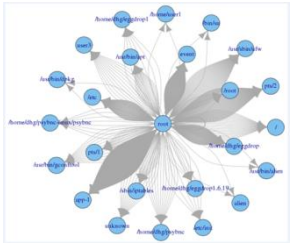
4. Accelerate toward security intelligence

Leaders adapt to handle new threats to the enterprise by developing threat-centered operations—developing a deep understanding of adversaries, their goals and techniques

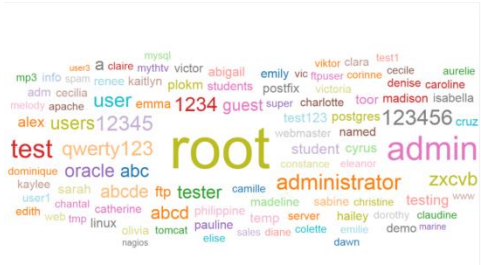
Leaders employ advanced analytics to deliver “context awareness”

- Leverage existing instrumentation in the enterprises with threat intelligence feeds and additional security event data sources to improve event triage and response performance
- Identify business initiatives / activities of interest to Threat Actors
- Incorporation of Threat Management teams in Security Monitoring & Response

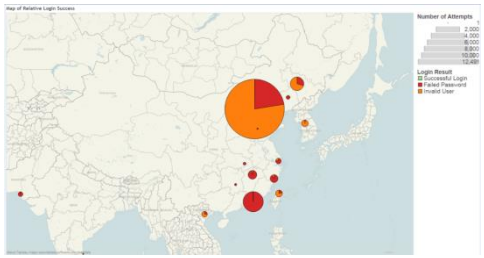
Example: Advanced security analytics provides visualization for rapid, active defense responses



File Touch Action Graph – a visualization of all of the file touch actions in a 24 hour window by the Root user on a suspected compromised web server



Common User Names – a visualization of the top 100 users names used in a brute force attack



Origins of attempts– a visualization of failed attempts by location

5. Develop end-to-end delivery and flexible sourcing strategies

Effective security organizations plan a delivery and operational strategy for each of the security services they offer

Considerations for Delivery and Sourcing:

- Determine which services to keep in-house vs. outsource to external provider
- Assess the enterprise's internal competencies for designing, building and deploying elements of a cyber-security program
- Justify sourcing decisions based on the overall risk tolerance, business case and commercial strategy based on security - business alignment
- Selecting partners that will help meet security-business goals
- Dynamic sourcing approach to address security coverage while helping leadership focus energy on active defense and proactive security capabilities and business enablement

Taking Action in Public Sector

Taking Action!

In industries worldwide, security leaders seek effective ways to improve their ability to defend against cyber security threats, reduce the risk of inadvertent data disclosures, achieve and maintain regulatory compliance, and ultimately enhance the value they deliver to their business counterparts and shareholders

Assessing current posture and adopting a business-aligned security strategy

Retain staff experienced with security architecture planning and design, tools and integration to drive successful outcomes

Establishing an end-to-end delivery capability, underpinned by a pre-integrated security solution set allows organizations to modularly select for their specific threat areas and adoption pace

Move to extract more value from the data they already collect and analyze

Create a clear and complete picture of defense strategies and synthesized security data can help security leaders to make rapid, intelligent security decisions based on business goals

Focus on managing the risk environment instead of concentrating strictly on compliance at the expense of strategically securing business growth, value and innovation

Security Leadership and Points of Contact

Security and Infrastructure Services Leadership

Kevin Richards
NA Security Lead

k.richards@accenture.com

Michael Montalto
NA H&PS Infrastructure Services Lead

michael.montalto@accenture.com

Lalit Ahluwalia
NA Public Sector Security Lead

Lalit.k.ahluwalia@accenture.com