NYS Cyber Security Conference

Enterprise Security on a Budget:
Deciding what gets done first and what doesn't get done at all

Kristine Briggs & Andy Hubbard

June 4, 2013

Agenda & Introductions

- Planning and Strategy
- Processes & Communications
- Risk Management
- Must Haves on Any Budget
- Cost/Benefit Trade-offs for Top Technologies
- Resources

© Neohapsis, 2013. Confidential.

Why is this the Agenda for Security on a Budget?

Planning and Strategy	To ensure alignment of business & security
Processes & Communications	To ensure the highest return on as little budget as possible you need a mature team and processes
Risk Management	To ensure decisions on budget items and project efforts are made in the context of risk
Must Haves on any Budget	To ensure security basics are all covered
Cost/Benefit Trade-offs for Top Technologies	To help with planning
Resources	To help with planning

© Neohapsis, 2013. Confidential.
NEOHAPSIS

Planning and Strategy

Key Principle #1

- **If you can't effectively communicate a security strategy and plan to the business, you can not ensure alignment**
- **If you don't have a <u>documented</u> security strategy and plan, get started!**

You May Have Some Assumptions

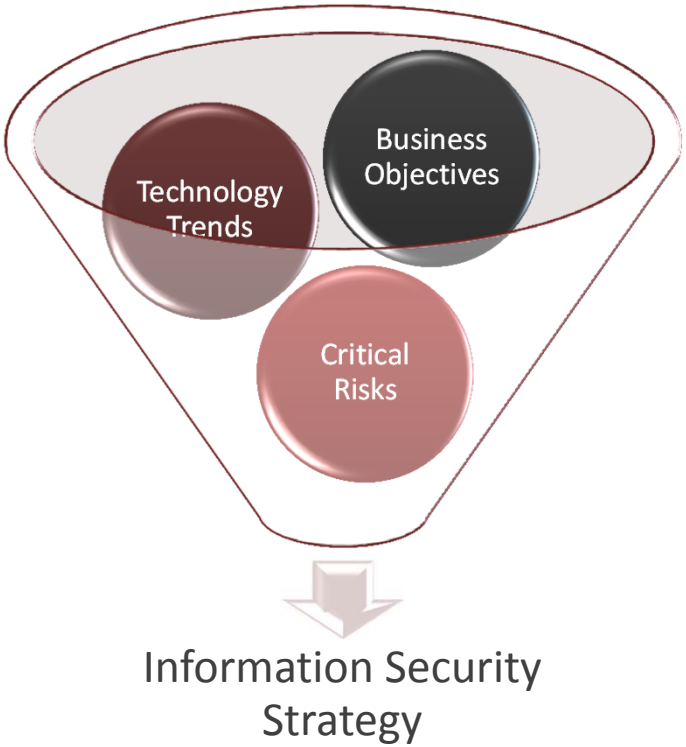
- Nod if this sounds correct:
  - Most people have more security budget than I do
  - My business goals are not aligned with my security goals which are not aligned with my budget
  - Most global companies have well developed security plans that they actually follow
  - Most large companies do security basics VERY well
  - Regulations are complex, constantly changing, and drive much of what I spend time on

- Which of these assumptions are true?

© Neohapsis, 2013.

Strategic Planning for Security

- Process of <u>setting priorities and focusing on them</u> with limited resources
  - Better to succeed at a few things than fail at many
- To support the organization's strategic objectives
- To address strategic risks and weaknesses
- To capitalize on opportunities
- To drive to execution and change



© Neohapsis, 2013.
NEOHAPSIS

Model #1: Rapid Strategic Planning

Business Objectives	Risks / Opportunities
Increased efficiency through mobility enablement	Data on unmanaged devices Data leakage in mobile apps
Expand to European markets	EU Data Protection Requirements
Reduce Fixed Costs	Redundant security operations

© Neohapsis, 2013.
NEOHAPSIS

Model #2: Detailed Strategic Planning

- Can be tailored to meet your company culture and communication styles
- Essential for managing with limited resources
- Communicates how security requirements are in support of the company's strategic objectives
- Supports more rapid capitalization on new technologies that can support desired growth (or greater attainment of mission, if a non-profit)
- Requires some level of discipline to develop and maintain

© Neohapsis, 2013.

Processes & Communications

Key Principle #2

- **You cannot do great things on a small budget without process and team excellence**

Characteristics of Under-Performing Security Teams

- Lots of “heroic” behavior
- No tie to longer-term department or company strategy
- No focus on planning, because:
  - “Plans always change”
  - “I don’t have the time”
  - ….
- Little understanding of basic risk management principles
- No metrics – inability to define success metrics and/or fear of being measured
- Inability to articulate the benefits of security
- Everything seems difficult
  - Fear of changes to the environment (even changes that improve security posture)
  - Change control becomes a tool to prevent required actions
  - Every action requires group consensus

 © Neohapsis, 2013.

NEOHAPSIS

Characteristics of High Performing Security Teams

- Business enablers - Not “If” but “How”
- Aligned to business strategy and risk tolerance
- Focus on top priorities, even if they are difficult
- Focus on process - technology is an enabling tool for process
- Once a risk is accepted, it’s accepted by all (don’t later say “I told you so…”)
- Continuous improvement is essential
- What gets measured gets done
- Sense of urgency and bias towards action
- Make and keep commitments and hold each other accountable
- Roles & responsibilities
  - Managerial economics 101 – assign tasks to the lowest cost resources in the organization that can successfully perform the task
  - Ensure roles and responsibilities are clear and well documented
  - Ensure process hand-offs are clearly defined (avoid the common “throw it over the wall” syndrome)
  - Ensure training is provided where needed

 © Neohapsis, 2013.

NEOHAPSIS

Communications

- Arguably, the most significant factor in effectiveness of an Enterprise Security Plan
- Effective communication promotes:
  - Understanding of security policies and procedures
  - Understanding of the expectations for end-users, administrative staff, vendors, contractors, and partners
  - Understanding of controls that are in place and the limitations of those controls
  - Understanding of the results of non-compliance (with policies, procedures, or regulations)
  - Inter-department/inter-group cooperation

 © Neohapsis, 2013.

NEOHAPSIS

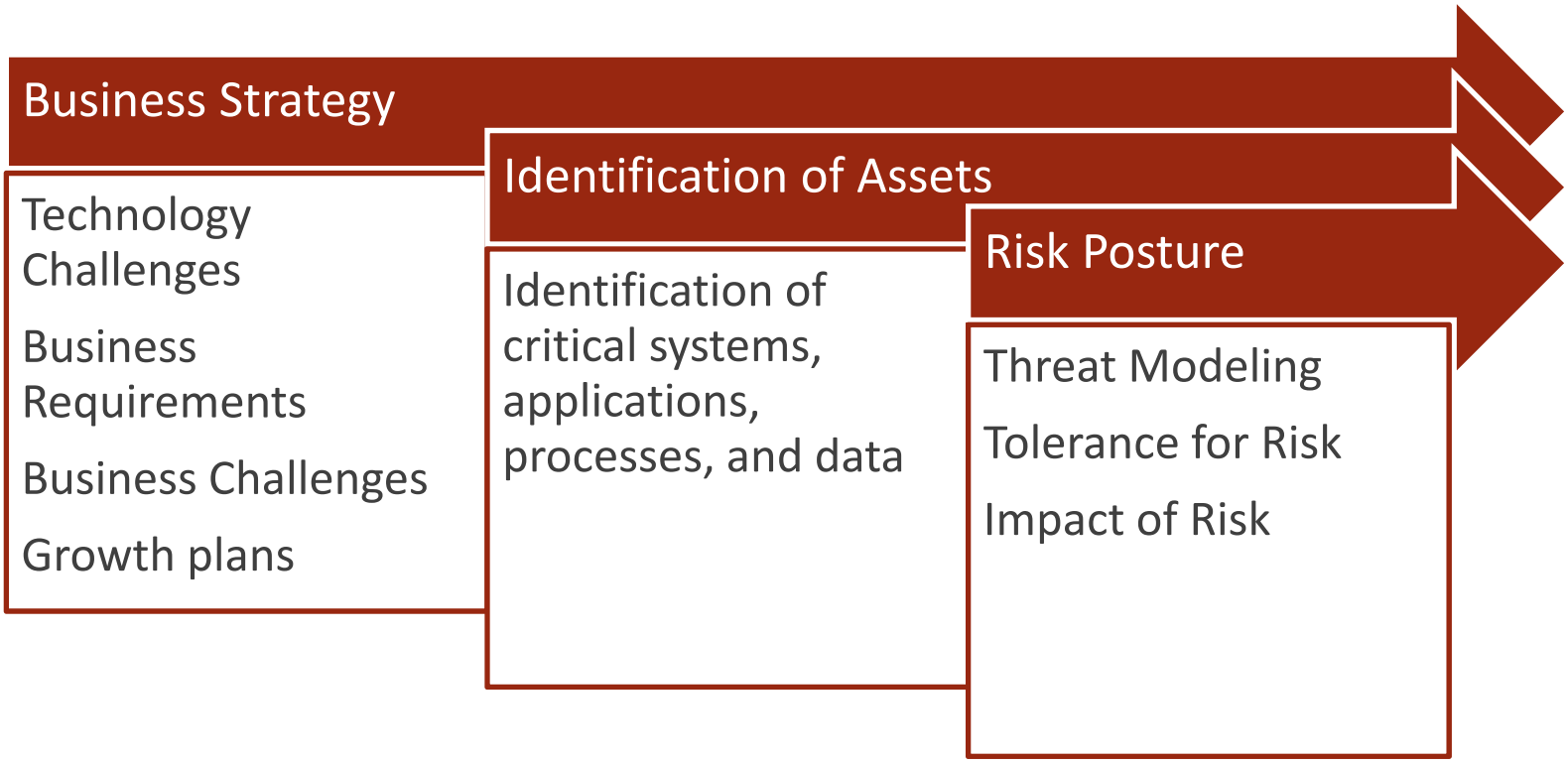
Risk Management

Key Principle #3

- If you don't have a framework for risk management, it's hard to make effective budget and resource trade-off decisions
- When done correctly, even a simple risk management process can facilitate business, IT, and security team alignment

Risk Management at a High Level

- What is Risk Management?
  - The Identification, assessment, and prioritization of risks and the application of resources to minimize, monitor, and control probability and impact of events.
- Components of a Risk Management Program

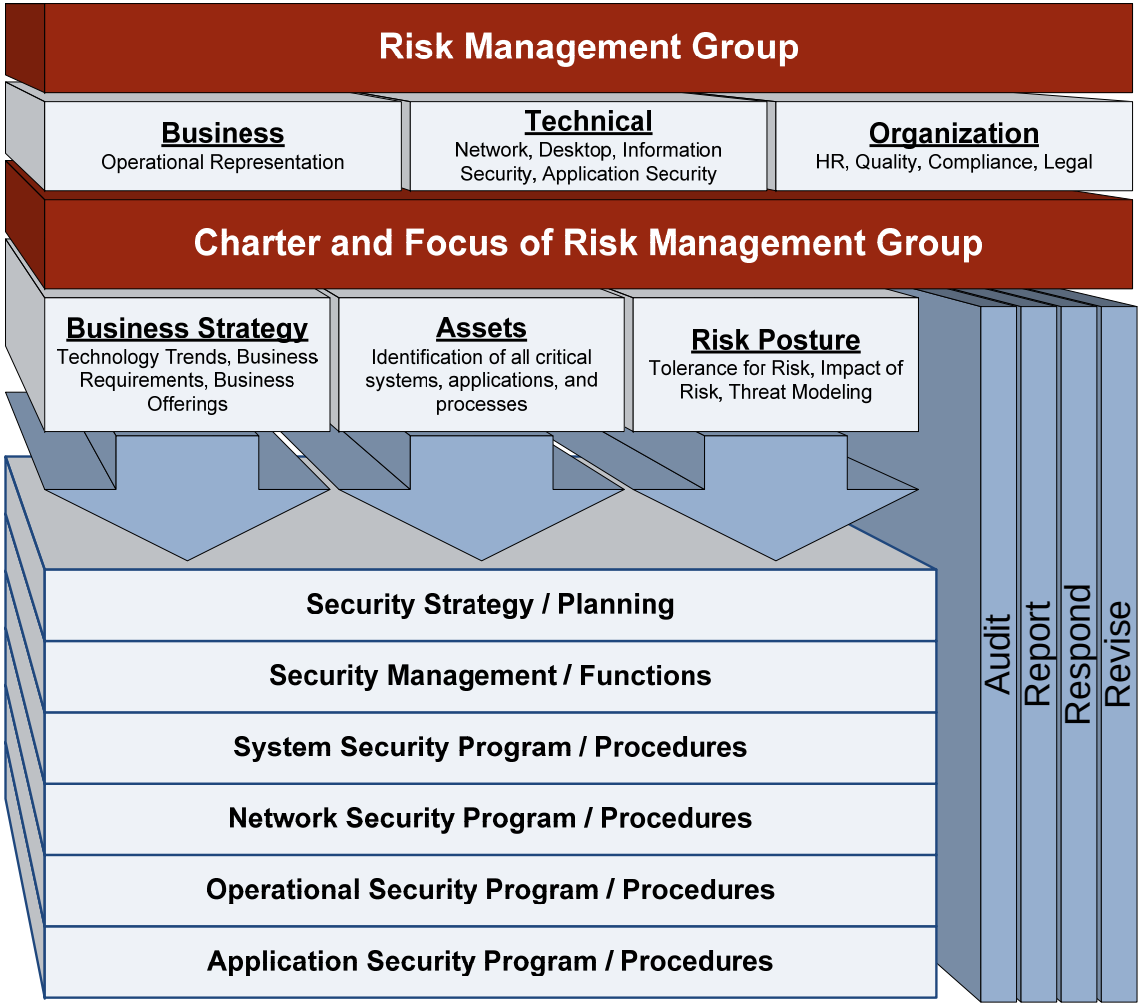


 © Neohapsis, 2013.

NEOHAPSIS

Risk Management

- Governance
  - Should be comprised of both technical and business unit stakeholders
  - Technical teams should only provide inputs to assess risk to the organization
  - Executive management must promote and support risk management initiatives



 © Neohapsis, 2013.

NEOHAPSIS

Risk Management – Getting Started

- LOTS of models to choose from
- Involves
  - Culture change
  - Process change
  - Management/Employee Awareness
- The best models have moved from detailed actuarial models to *action based* models
- Common Issues:
  - Not clearly tying technical risk to (potential) business impact
  - Starting too big and complex
  - Asking business unit leads to sign off on technical risks they don't understand

 © Neohapsis, 2013.

NEOHAPSIS

Must Haves on Any Budget

Key Principle #4

- If you are managing a security program on a tight budget, you must ensure you have defined the most essential items to be covered within that budget; this will vary somewhat for each organization

Must-Haves on any Budget

- Governance and Support from Senior Executives
- Effective Security Policy
- Published Technical Standards
- Trained Information Security Personnel
  - Mandatory Continued Education
  - Effective Security Awareness (the work force supports your security team)

Fundamental Technical Controls

- Perimeter Defenses (Firewalls, Access Controls, Threat Detection)
- Secure Build
- SPAM and email content control
- Network Segmentation and Isolation of Critical Assets
- Patch Management
- Anti-virus, Anti-spyware, and Anti-malware
- Data Leakage Protection / Internet Access Control

 © Neohapsis, 2013.

NEOHAPSIS

Must-Haves on any Budget

- Effective security assessment and remediation
  - Exception processes
  - Standard remediation processes
  - Regular reporting of security efforts, findings, and issues to senior leadership
- Integration and regular communication between:
  - Regulatory Compliance
  - Legal
  - Information Security
  - Internal Audit

 © Neohapsis, 2013.

NEOHAPSIS

Must-Haves: Metrics

- Advice for starting to develop metrics:
  - JUST GET STARTED – something is <u>always</u> better than nothing…
  - … As long as its meaningful (don't measure just because you can)
  - Metrics must be consumable…less is often more valuable
  - Quantitative data often becomes even MORE useful with some qualitative commentary
  - "Good Metrics" answer key management questions and facilitate decision making
    - Am I comfortable with level of risk?
    - Am I getting better or worse?
    - Am I out of bounds of defined tolerances?
    - Do I need to take action?
  - Trending over time can be valuable to show a clear result or provide actionable information
  - Get help if you need it

A Tale of 2 Metrics

Average number of vulnerabilities per system
- Too many variables limits trending (fluctuates based on number of new vulnerabilities)
- Poor indicator

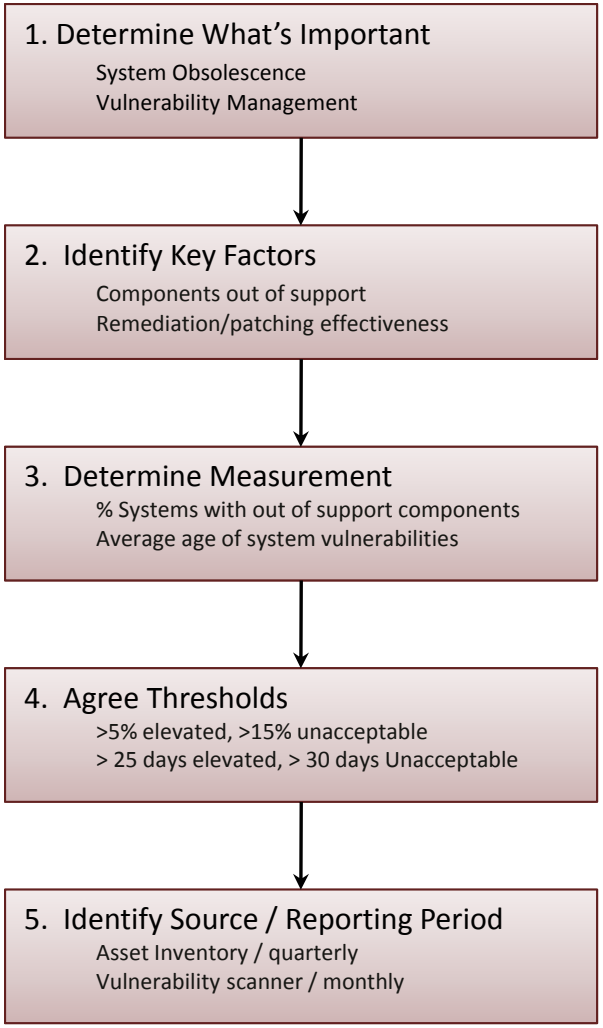
Average age of critical vulnerabilities
- Limited variables
- High trending potential
- Good indicator

 © Neohapsis, 2013.

NEOHAPSIS

Must-Haves: Metrics

- How to get started:
  - Identify significant risks or key performance indicators to monitor; monitoring "everything" is not practical
  - Determine 1 or 2 meaningful factors to monitor for each
  - Different indicators will have differing measurements and reporting periods (daily, monthly, quarterly, annually)
  - Thresholds should reflect risk tolerance
  - Sometimes meaningful metrics are harder to collect than accessible data; the cost/benefit for each metric should be considered
- Having defined Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) is important as the security program matures



 © Neohapsis, 2013.

NEOHAPSIS

NEOHAPSIS

Cost/Benefit Trade-Offs for Top Technologies

Key Principle #5

- If you don't manage your technology vendors very tightly, you will find an ever-increasing percentage of your budget going to hardware and software
- This should be managed in a STRATEGIC fashion, not with the attitude that "purchasing will handle it"

Cost/Benefit Trade-Offs for Top Technologies

- Key questions
  - Does your organization focus on retention of talented IT staff?
  - Are you ready to re-think classic security roles?
  - Who will manage your out-sourced and cloud-based security solutions?
  - Are you aligned to actually use the key benefits of top technologies?
    - Have you thought through the use of key features?
    - Have you considered how the new technologies will affect core processes?
    - Do the new features violate an existing corporate policy (e.g. will you actually be allowed to use what you've paid for)?
    - Do you control what your users do, what they access, how they connect, when they can connect?
    - Do you care what your users are accessing and can you identify individual users?
    - Do you train them appropriately?
    - Do you establish relationships with your most important vendors, so you can influence their roadmaps?
    - Do you look at logs and reports?
    - Can you prevent users from bringing their own devices?

 © Neohapsis, 2013.

NEOHAPSIS

Cost Reduction Techniques

- How do these fit into your strategy?
  - Cloud infrastructure
  - SaaS for core business applications
  - Outsourced management and support

 © Neohapsis, 2013.

NEOHAPSIS

Resources

Resources

- SANS
  - http://www.sans.org/security-resources/
- NIST
  - http://csrc.nist.gov/
- Cloud Security Alliance
  - https://cloudsecurityalliance.org/
- ISO
  - ISO 27001/27002: Info Sec
  - ISO 31000: Risk Management
  - ISO 22301: Business Continuity

 © Neohapsis, 2013.

Summary of Key Principles

1. Ensure you have a documented security plan that aligns security goals to business goals
2. Strive for a top-tier team with mature processes; make every FTE count and leverage process automation as much as possible
3. Work toward mature risk management processes, so budget and technology trade-off decisions can be made in the context of risk
4. Metrics may seem daunting, but are critical to decision making and budget justification
5. Define the "must-haves" for your program and ensure they are in place
6. Take time out for strategic thought and continuous improvement

 © Neohapsis, 2013.

NEOHAPSIS

Thank you

 © Neohapsis, 2013.

NEOHAPSIS

Supplemental Slides:
Detailed Guidance in Key Areas

- Strategic Planning
- Considerations for Top Technologies
- Must-Haves on a Budget

 © Neohapsis, 2013.

NEOHAPSIS

Detailed Guidance in Key Areas: Strategic Planning

 © Neohapsis, 2013.

NEOHAPSIS

Plan Development: Key Questions

- ✓ What are the most critical major business imperatives am I responsible for supporting – now and in planning?
- ✓ What are my critical assets?
- ✓ What are my real threat sources?
- ✓ What is my total security budget?
- ✓ Am I meeting my compliance requirements?
- ✓ How do I keep up with quickly evolving threats?
- ✓ Are my applications secure?
- ✓ How do I ensure I am using my security budget most effectively to address my top risks?
- ✓ How can I effectively and securely leverage mobile and cloud applications to enable business growth?
- ✓ Should I be more aggressively leveraging cloud-based services for lower net cost, effortless upgrades, and payment based on use?

 © Neohapsis, 2013.

NEOHAPSIS

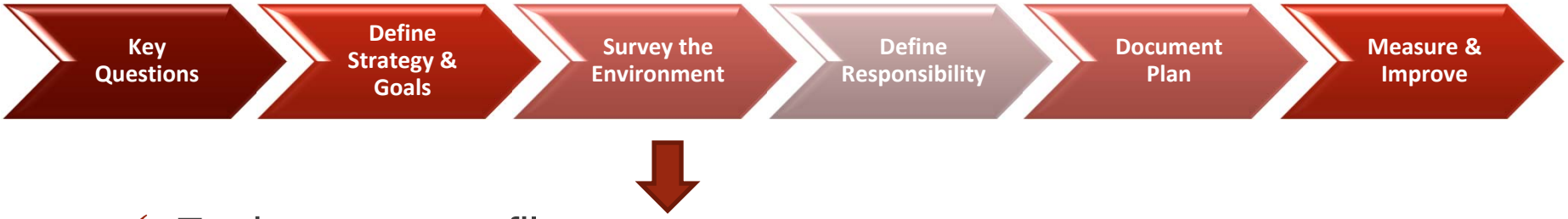
Plan Development: Define Strategy & Goals

- ✓ Understand and effectively support top business initiatives and goals for growth
- ✓ Establish/improve the information security infrastructure using best practice to secure network and computing environments
- ✓ Ensure confidentiality, integrity, and availability of computing resources and data
- ✓ Support Corporate initiatives and strategic technology plan
- ✓ Prevent abuses of computer and network resources
- ✓ Ensure compliance with regulations and standards
- ✓ Promote standardization of security practices and policies
- ✓ Protect brand and reputation
- ✓ Prevent incidents that may affect customers or staff
- ✓ Promote security awareness
- ✓ Protect the privacy of customer data
- ✓ Save money and/or drive business growth

 © Neohapsis, 2013.

NEOHAPSIS

Plan Development: Survey the Environment



- ✓ Environment profile:
  - Heavily regulated?
  - Requires connectivity from disparate resources?
  - Must allow uncontrolled devices access to my network and resources?
  - Utilizes a remote workforce?
  - Makes heavy use of mobile or cloud computing?
  - Provides services to external resources?
  - Relies upon connections to partners or vendors?
  - Previously an attack target?
- ✓ Do you have an IT security strategy or plan?
- ✓ Do you have documented technical and security standards?
- ✓ Can the information security group influence technical decisions?

 © Neohapsis, 2013.

NEOHAPSIS

Plan Development: The “G” Word

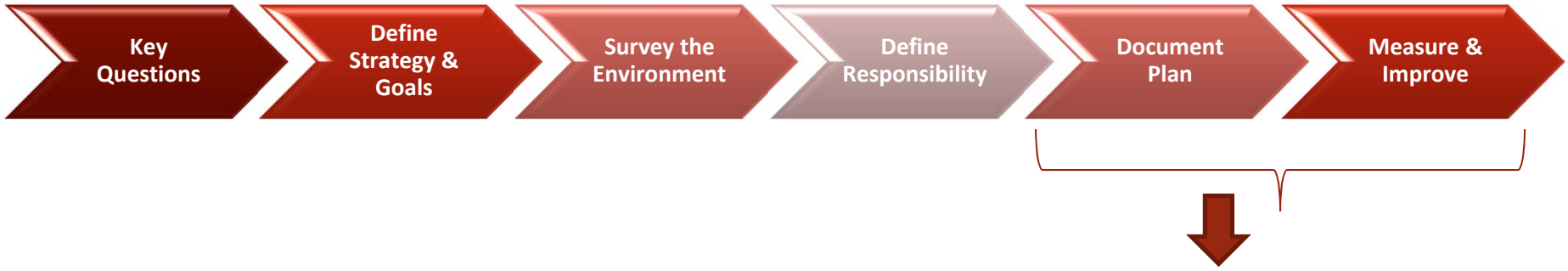
What Is GOVERNANCE?

Who is responsible for:

- ✓ IT governance
- ✓ Security governance
- ✓ Regulatory compliance
- ✓ Risk management
- ✓ Corporate communications
- ✓ Defining corporate risk appetite
- ✓ Security management
  - Systems security
  - Network security
  - Operational security
  - Application security

© Neohapsis, 2013.
NEOHAPSIS

Plan Devt: Document, Measure & Improve



- ✓ Review the environment and identify what must be protected
- ✓ Identify restrictions you must operate within (budget, regulatory, internal compliance)
- ✓ Select technical, operational, and procedural tools that will have the greatest effect
- ✓ Avoid policy, procedural, or technical controls that are inefficient or cannot be enforced
- ✓ Define requirements to enforce controls that will provide a benefit to the greatest number of systems
- ✓ Define incident response and recovery
- ✓ Define metrics & continuously improve

 © Neohapsis, 2013.

NEOHAPSIS

Detailed Guidance in Key Areas: Considerations for Top Technologies

 © Neohapsis, 2013.

NEOHAPSIS

Considerations for Top Technologies

Best Practice Wisdom

- Firewalls
- Spam and e-mail content control
- Anti-virus, anti-spyware, anti-malware
- Patch management
- DLP
- SIEM
- IDS/IPS
- Mobile security and BYOD
- Cloud technologies & platforms

 © Neohapsis, 2013.

NEOHAPSIS

Considerations for Top Technologies

Firewalls

- Required technology for regulatory compliance
- Cost is fairly wide ranging
  - Range from $75 to over $50,000 per device
  - Small business solutions are available for $2-$5k
  - Can get very interesting feature bundles with modern firewalls (AV/AS, Threat Monitoring, Application Filtering, Content Control)
- Role-based access
  - Most of the modern user interfaces are fairly easy to use
  - Move some of the firewall duties to network or desktop support
  - Integrate threat reporting with your NOC or Support Center
- Consider outsourcing support (risk vs. FTE cost)

 © Neohapsis, 2013.

NEOHAPSIS

Considerations for Top Technologies

SPAM and Email Content Control

- Not specifically required by regulations, but recommended
- Generally cost per seat, or can purchase devices
- Cloud-based solutions offer lower cost and provide other services
- Based on solution/vendor costs range from $1-10 per user (more for additional features)
- Caching/store and forward in the event of a local mail server outage
- Filtering before the email even hits your environment
- Additional costs
  - Need administrators that understand email and filtering
  - Plan on at least .5 FTE – rule management, email release
  - Granular controls for certain SPAM events may require more configuration time (plan on multiple per month)

© Neohapsis, 2013.

Considerations for Top Technologies

Anti-virus, anti-spyware, anti-malware

- Required technology for regulatory compliance
- Strong candidate for cloud-based solutions
- Clients must be able to interact with the server
  - Management
  - Updates
  - Reporting
- Consider using solutions bundled with your OS (Microsoft)
- Consider in-line AV/Threat protection offered from edge devices
  - Layered security
  - A second chance to detect subverted devices
- Organizations at +-10,000 workforce members will generate ~1,200 virus events per month. Plan on 1 FTE per month in remediation.

 © Neohapsis, 2013.

NEOHAPSIS

Considerations for Top Technologies

Patch Management – required technology for regulatory compliance

- Expense is related to distribution/scanning solution and even more, the number of FTEs required to contribute to the process
- Several solutions integrated with, or easily bolted onto, the OS
- Several cross-platform solutions
  - More expensive and more complex
  - Greater requirement of FTEs to manage
- Patch Management includes delivery, distribution schedule, reboot schedule, and testing processes
  - This requires strong communications between patch management groups and the analysts responsible for testing systems after patches have been applied
- Plan on at least 2 FTEs for distribution alone
  - Server and workstation distribution should be separate as they are generally separate distribution cycles
  - Patch testing (and recovery processes) are also different

 © Neohapsis, 2013.

NEOHAPSIS

Considerations for Top Technologies

Mobile Security and BYOD

- Not specifically required by regulations (unless you are focused on data protection)
- Technology still in its infancy
  - Solutions focused on device control, not data control
  - Current solutions not ideal for multi-environment enforcement
    - What happens when a user must work within multiple environments that try and enforce Mobile Security policies?
  - Legal complications - corporate versus private data residing on the same device.
  - Less expensive solutions provide less control and have limited functionality across mobile platforms
- Hidden costs of BYOD
  - Helpdesk/support, multi-device support, Data loss (data management), profile management and feature support.
  - Plan on at least .5 FTE for this continued support.

 © Neohapsis, 2013.

NEOHAPSIS

Considerations for Top Technologies

IDS/IPS

- Not specifically required by all regulations, but recommended
- Typically sold per device, although per-node solutions exist
- The technology costs are significantly outweighed by support costs – plan on .5 to 1 FTE for IDS (depending on extent of deployment)
- Strong candidate for managed services solution (especially when considering 24x7 support)
  - Requires strong security background to manage and maintain
  - Tuning, updates, management are critical
  - Little benefit in scenarios where traffic is encrypted (must terminate the encrypted session to examine traffic)
  - IPS solutions require some methods of getting in-line with traffic (to intercept and terminate connections)
- Cloud-based solutions are typically focused on user control (not classic IDS/IPS).

 © Neohapsis, 2013.

NEOHAPSIS

Considerations for Top Technologies

Putting it all together

- If you were to invest in all of these solutions, plan on staffing at least 5 people across your ITS organization (depending on department responsibilities).
- This assumes an organization of between 500 – 2,000 servers, and a limited web presence.
  - Firewall, IDS/IPS 1 to 1.5 FTE
  - SPAM control, etc. .25-.5 FTE
  - Patch Management 2 FTEs
  - AV/Remediation 1 FTE
  - BYOD /.25-.5 FTE
- This does not take into account other requirements, such as:
  - Networking
  - Remote access/VPN
  - Server Build

 © Neohapsis, 2013.

NEOHAPSIS

Detailed Guidance in Key Areas: Must-Haves

 © Neohapsis, 2013.

NEOHAPSIS

Must-Haves on any Budget

Fundamental Security Controls

- Perimeter Defenses (Firewalls, Access Controls, Threat Detection)
- Secure Build
- Data Leakage Protection / Internet Access Control
- SPAM and email content control
- Secure email

 © Neohapsis, 2013.

NEOHAPSIS

Must-Haves on any Budget

Perimeter Defenses (Firewalls, Access Controls, Threat Detection)

- Network Segmentation
- Isolation of Critical Assets
- Control of access to data

Secure Build

- Reduce the attack surface (remove unnecessary software and components)
- Patch Management (OS and relevant software)
- Anti-virus, Anti-spyware, and Anti-malware

Data Leakage Protection / Internet Access Control

- Control of end-user access to data within the organization and data outside of the organization

© Neohapsis, 2013.

Must-Haves on any Budget

SPAM and eMail content control

- Email and web browsing are still the top threat sources for most businesses
- 72-76% of email is SPAM with about 3% of that containing malicious content
- Even with content filters in place, about 19% gets to user inboxes
- Email is still a significant avenue for confidential data to exit the organization

Secure eMail

- Users routinely expose the organization to risk by inadvertently sending confidential data via unsecured email
- Many organizations require secure email in order to do business
- There are so many options available – choose the one that best fits your use cases

© Neohapsis, 2013.