Technology and Business Risk Management:
How Application Security Fits In

Pete Perfetti
IMPACT Security, LLC
pperfetti@impactsecurityllc.com

OWASP
LASCON 2010
Ausitin, Texas
29 October, 2010

The OWASP Foundation
http://www.owasp.org

Presenter's Background

- Former head of IT Security and Risk Management at global financial and entertainment companies.
- *"The Visible Ops Handbook - Starting ITIL in 4 Practical Step*s" – Work at Viacom and MTV was one of the case studies on how to successfully achieve a high performing IT organization.
- *"The Visible Ops Security Handbook – Achieving Common Security and IT Operations Objectives in 4 Practical Steps"* – Contributor, wrote end of chapter summaries for each section of the book.
- "*Change, Configuration, and Release Performance Study*" – IT Process Institute
- "*Top Performer Roundtable to focus on Change Configuration and Release practices that drive highest levels of performance*" – IT Process Institute
- Emerging Trends in Enterprise Security - **"***Corporate Challenge: INFORMATION SECURITY@RISK: ARE YOU ON THE RISK MANAGEMENT TRACK?"* - Technology Managers Forum
- Former OWASP Chapter Leader: NY/NJ Metro Chapter

Current Activities

- IMPACT Security, LLC
  - Cyber Security Consulting & Professional Services Firm
  - Vulnerability & Risk Assessments; Penetration Testing
  - Developing and/or Enhancing Information Security & Risk Management Programs
  - Incident Response, Prevention, and Recovery
  - Audits, Compliance Checks (SOX, PCI, etc.)
  - Tactical and Strategic Cyber Security Projects
    - Security, Audit, and Risk Management Training
    - Remediation, Implementation
  - Dallas, Texas; and NYC Metro Area
    - Financial, Entertainment, Media, Sports, Publishing, Pharmaceutical, Oil & Gas, Aerospace, Government, Academic, Retail, Individuals
- OWASP Project – CISO Application Security Checklist

Information Security Officer

and

Risk Manager concerns.

Primary Types of Risk Concerns and their Business Impact

- **Operational** – Adverse affects on the operational stability of the organization's technology infrastructure that compromises the confidentiality, integrity, and availability of data and services.
- **Financial** – Direct financial loss to the business.
- **Reputational** – Harm done to a company that may not be reversible, and may cause direct or indirect negative financial impact.
- **Legal** – Issues that cause criminal or civil legal problems for the organization, or that force compliance with laws and court ordered directives. This type of risk can often lead to other types of risks.
- **Strategic** – Issues that put the firm on a course for future legal, financial, reputational, operational risk.

How does this affect applications?

Survey of Risk Managers

- What are your three primary risk concerns regarding applications and what is the impact of these application risks on your business?

Survey of Risk Managers

- What are your three primary risk concerns regarding applications and what is the impact of these application risks on your business?
- What are your top three issues or concerns for overall audit and compliance?

Survey of Risk Managers

- What are your three primary risk concerns regarding applications and what is the impact of these application risks on your business?
- What are your top three issues or concerns for overall audit and compliance?
- Top risk concerns for application security were almost identical to those for overall audit and compliance and meeting business risk objectives.

Primary Risk Concerns Regarding Applications and Risk to Business

- Top risk concerns for application security were almost identical to those for audit and compliance.
  - Effective and Efficient Change Control.
  - Appropriate and Effective Access Control
  - Lack of a comprehensive Risk Assessment process
  - Adherence to the SDLC
  - How an application affects other areas of the business, & are the other business areas consulted in the design & development of new code, and involved in testing and approvals.
  - Failure to assess risks to third party or purchased applications, their connectivity, understanding how the application will work within the existing security systems & compliance requirements.
  - Up to date policies and documentation that appropriately define risk tolerance.

Effective and Efficient Change Control

- Impact of changes, including patches, to the applications on stability and security not understood or documented.
- Process is too complex and not auditable.
- Lack of effective enforcement of Change Control policy and process.
- No effective way to measure change.
  - Has something changed?
  - Was the change authorized and scheduled?
  - Number of successful vs. unsuccessful changes.
  - Is the change compliant with policy?
  - Were all approvals obtained?

Appropriate and Effective Access Control

- Approvers don't fully understand the business processes and the objects they are approving access to.
- Inadequate User Access Rights Reviews.
- Inadequate or undocumented data classification.
- Access to data is not controlled or monitored.

Lack of a Comprehensive Risk Assessment Process and Adherence to the SDLC

- Lack of stability from non-adherence to the SDLC
- Lack of a documented development process with adequate security and risk assessments included which leads to, or is a product of:
  - Poor security design
  - Segregation of Duties issues
  - Inappropriate access to privileged functions and sensitive data
  - Inadequate testing and approval by the business
- Failure to correct security issues prior to moving code from one stage to another.
- Lack of, or failure to adhere to, a formal development framework and set of processes.

Checklist: Considerations for Application Development

- Issues with new in-house application development:
  - How does the application affect other areas of the business?
  - Are all areas of the business considered in the design and development of the new code?
  - Are the other business areas involved in testing and approvals? (Extends to the Change Management process)
  - Does the process adequately consider and assess risk prior to development?
  - Is sufficient consideration to integration with the rest of technology infrastructure sufficiently undertaken?
  - Is there a failure to correct the stability, security, and risk issues prior to code release, implementation, and other changes?
  - Are all policies, standards, and processes up to date and is the application compliant?

Checklist: Considerations for Application Acquisition

- For applications purchased from a third party:
  - Is consideration given to how the application will work within the current security architecture?
  - Has a security and risk review been conducted on the workflow?
  - Will the new application add new entry points?
  - Does it meet requirements for authentication, access control, and other policies and standards?
  - Will the application only read data, or will it write it?
  - What is the classification of that data?
  - Who needs to access the data?
  - What is the authentication mechanism?
  - How will we perform audits, assessments, and monitoring to prove compliance and maintain business and risk objectives ?

Obstacles to Audit, Compliance, and Application Security

Obstacles to Effective Audit and Compliance in Application Security

- Resistance to correcting the root causes that cancels out efficiency and cost effectiveness, and increases risk. Audit findings are frequently repeated unnecessarily.
  - telnet, ftp, sql injection, etc., are all still with us.
- IT is, or will be, caught in the audit-to-audit cycle and possibly the break/fix cycle as well.
- Lack of communication & interaction, or there is rivalry between different groups within IT which negatively affects risk and the business.
- Failure to understand risk causes Management, IT, and Audit to make erroneous decisions.
- Failure to assign owners to applications and issues, and for those owners to responsibly address all findings.

Obstacles to Effective Audit and Compliance in Application Security

- Auditors are perceived as adversaries – ISO/RMs and other security folks are to a lesser extent.
- Resources are strained gathering data and responding to findings – An audit adds to support and dev issues:
  - It's a big distraction from the daily routine.
  - But the break/fix cycle is also a big distraction
- Always seem to be finishing one audit - or not - when the next one starts. Because:
  - The root causes are not being addressed, and;
  - The process for correcting them is not efficient or effective.
- Not all companies have standards for responding to audit findings and closing them out.

Obstacles to Effective Audit and Compliance in Application Security

- Inadequate functionality and processes built into the application cause many findings, such as monitoring, auditing, logging, access control, SoD, etc.
- Rush to implement without considering the security and risk implications, and the compliance requirements.
- Inadequate, infrequent, and inconsistent security and risk reviews and failure to correct security and risk issues prior to implementation or deployment.
- Policy Issues
  - Policies are not in tune with regulatory and legal obligations.
  - Staff are not aware of, or are just disregarding, policies.
  - Policies do not accurately reflect Mgt's Actual Risk Tolerance.

How do these problems arise?

How the Problems Arise

- Many times concerns are focused on immediate issues:
  - SLA - Deadlines that have to be met
  - General support issues, e.g. firefighting, break-fix cycle
  - Unresolved and repeat audit findings still exist
- You cannot maintain control if you don't know and understand what's going on.
- The same problems are always with us because we have lost situational awareness and control.
- You lack the will to resolve the issues at the root cause.

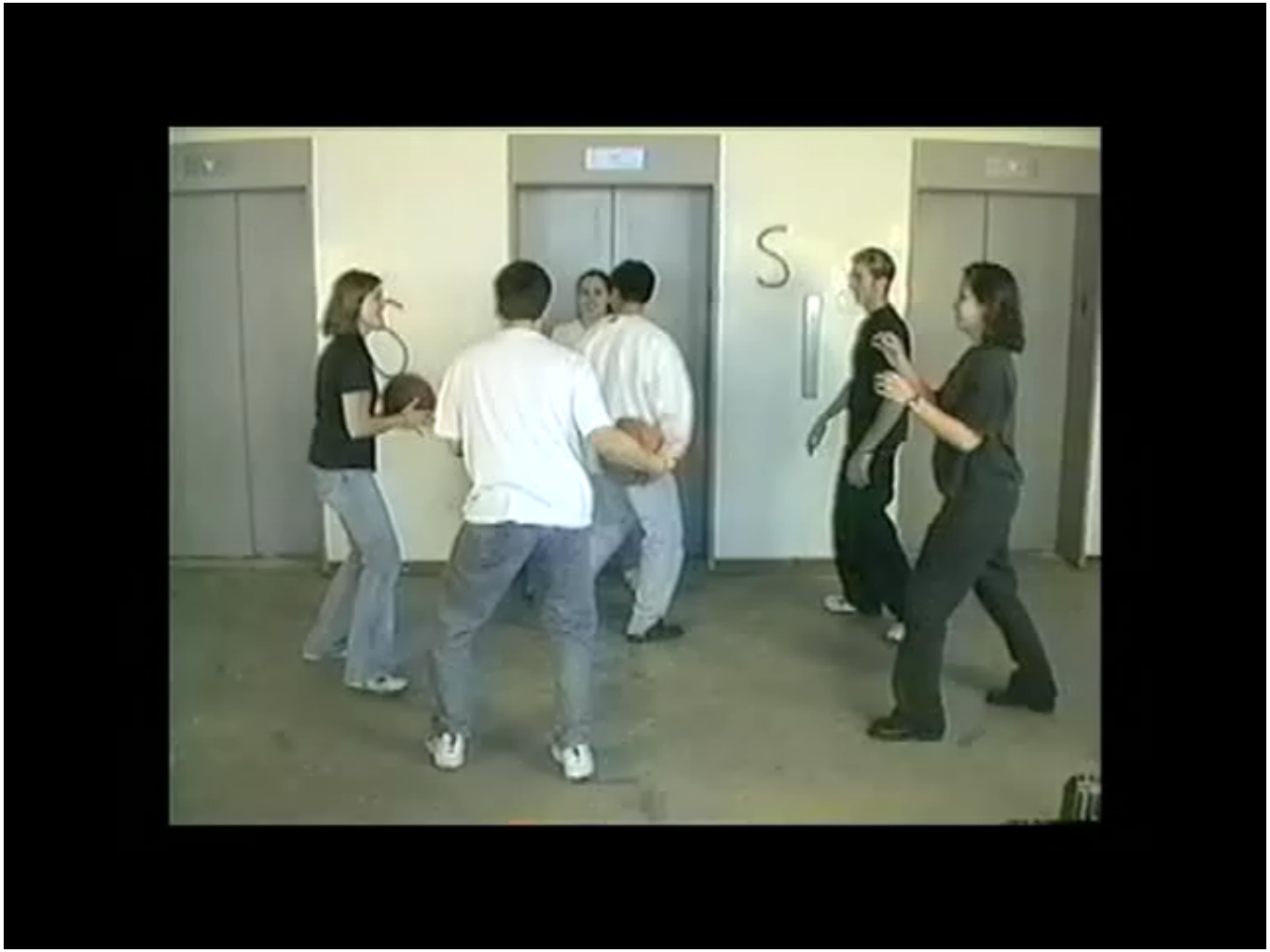
Situational Awareness

Movie Time

Situational Awareness

Our concern is how many times the team in white passes the ball.

How many times does your team pass the ball?



How many times did the gorilla beat his chest?

So how did you miss this?

If you didn't see the gorilla…

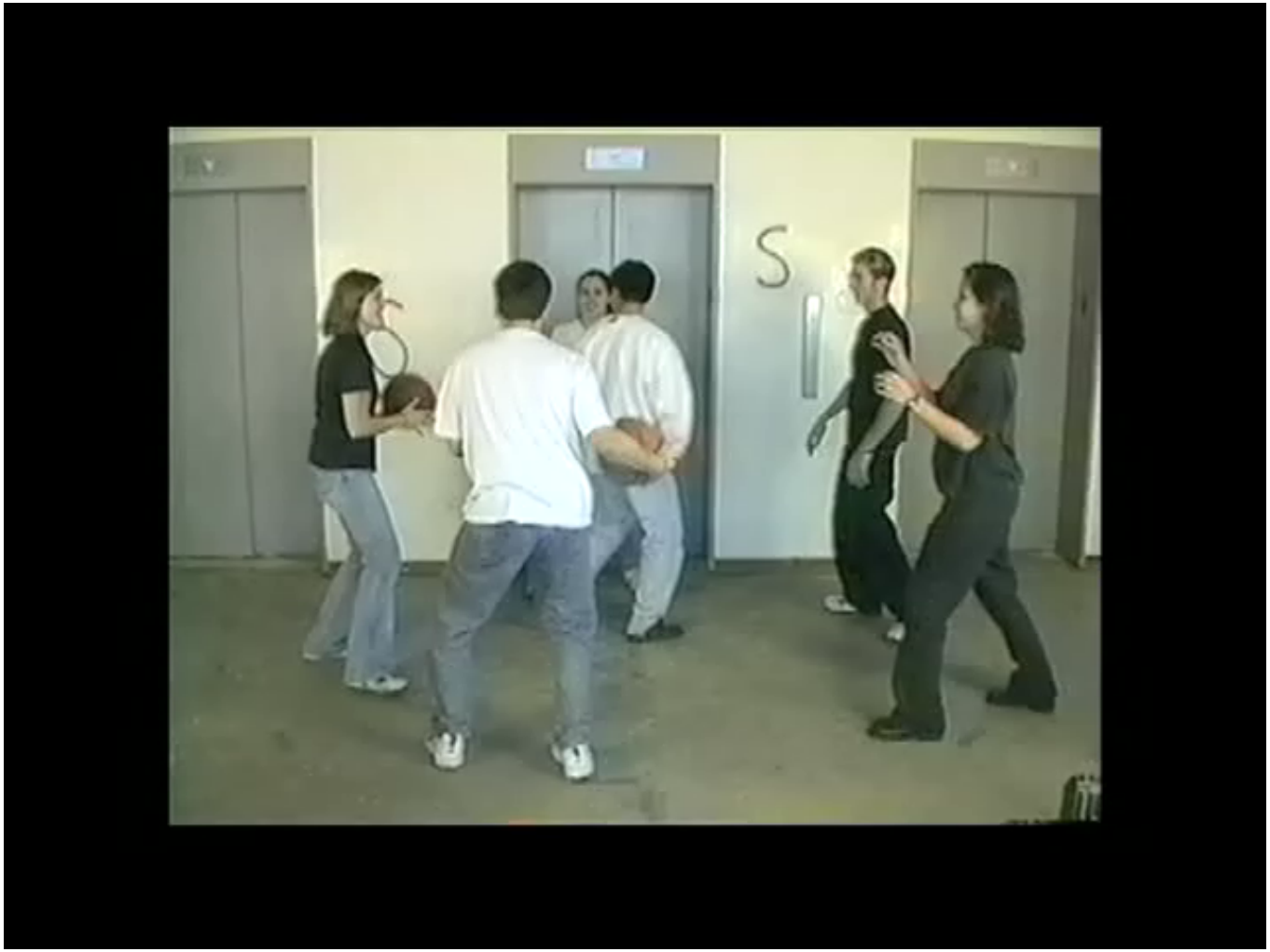
- ~75% of people don't see it.
- You were too focused on your individual task that you failed to see the anomaly.
- Others were too focused on what they were told to do, and they also missed it.
- You also missed what the other team was doing.

For the people who saw the gorilla …

- Do you know how many times the gorilla actually beat his chest?
- Do you know how many times the team you were supposed to watch actually did pass the ball?
- How many times did the other team pass the ball?

Movie Encore

How many times does the team in white pass the ball?



Specifics of How We Lose Situational Awareness in Technology

Examples of Poor Situational Awareness and Loss of Control

- **Change Management** - Little to no effective Change Management.
  - Process is too complex or too difficult to follow so it is bypassed.
  - Micromanaged approvals stifle efficiency and effectiveness.
  - No ability to effectively audit or report on important metrics.
  - Changes to infrastructure can not be made without major risk to stability *(The infrastructure is too fragile).*

Examples of Poor Situational Awareness and Loss of Control

- **Access Control** - You don't know who has access to data.
  - There is little or no classification of data, no documented owners, nor are there reviews of user access.
  - Approvers have no understanding of what they are approving access to or for.

Examples of Poor Situational Awareness and Loss of Control

- **Adherence to the SDLC** - The risk assessment process does not exist or is not enforced.
  - Application risks are not understood by Management, Business Owners, or Developers.
  - Applications are not adequately addressing risk in Policies, Standards, and Processes.
  - Risk assessments are expected to be conducted immediately prior to production release leaving no time to correct any issues.
  - Risks are not reviewed prior to development or acquisition and are discovered after implementation.

Examples of Poor Situational Awareness

- **Documentation** - Risk Tolerance as documented in policy does not match the risk that top level management is willing to take.
  - Missing or outdated versions of policies, processes, guidelines, standards.
  - Little or uneven enforcement of policies, standards, processes.
  - Monitoring and auditing is not defined adequately.

Examples of Poor Situational Awareness

- **Monitoring** - No relevant monitoring or centralized review.
  - Monitoring the wrong data for your environment.
  - Bad things are happening and no one understands why.
  - You don't know if bad things are happening.

How to fix things.

Breaking the Audit and Compliance Cycle

- **NECESSITY**
  - Accept and understand that these things are necessary. Don't tolerate excuses for not getting things accomplished. Find solutions to the root causes.
- **ALLIANCE**
  - Make Internal Audit and Security/Risk Mgt. your allies not your adversaries. Work as a team to resolve and reduce findings that the external auditors and regulators might discover.
- **DOCUMENTATION**
  - Ensure that your policies, procedures, and standards are accurate and appropriate, and that your risk tolerance is properly defined in policy. Understand the business objectives and legal obligations when reviewing, updating, or creating your policies.

Breaking the Audit and Compliance Cycle

- **DESIGN**
  - Ensure audit & compliance are built-in to your applications, databases, systems, and acquisition.
- **ROUTINE**
  - To improve efficiency, cost effectiveness, reduce aggravation and free up resources, auditing and compliance testing should be just like pushing a button to get the data you need. Make everything routine.
- **BUSINESS CASE**
  - Define your arguments around business needs and managing business risk for everything from budgeting to audit and compliance response.

Breaking the Audit and Compliance Cycle

- **METRICS**
  - Incorporate as many *valuable* and auditable metrics as you can into routine monitoring and reporting.
  - Metrics need a context in order to add any value.
- **REPORTING**
  - Ensure that policy appropriately defines what has to be monitored and by whom. – *Use the data to generate a monthly report of how you are doing e.g. "Monthly Risk Mgt" report that contains only relevant metrics along with recommendations*.
- **POLICIES**
  - Adapt your policies, procedures, and standards to facilitate auditing and monitoring. Keep them updated according to changes in threats, risks, compliance, and business needs.

A few quick facts about Change Management.

The Importance of Change Management

- Most often overlooked in IT in its importance and detail.
- Superb Change Management is the most common trait in high performing IT organizations according to a study by the IT Process Institute and documented in the Visible Ops series of books.
- It's the root cause of many audit and compliance issues.
- It helps you maintain situational awareness of the infrastructure.
- Works best when it is practical – Only include the most important criteria and approvals in the process to ensure that it is effective.

Change Management Tips For Applications

- All changes must be reviewed for compliance to policy.
- All changes tracked and monitored for successful vs. unsuccessful changes.
- Self-audit the process, including proper approvals.
- Change control processes might need to be defined separately from OS, Network Devices, DB, etc., as the processes and risks of the changes may be different.
- Remove self-promotion from one environment to the next.
- Obtain approvals before the change is moved to the next area, e.g. dev to qa, then qa to prod.
- Everyone must follow the processes.
- Make sure the Business/App Owners know what you're doing and that they are included in the Change Management process.

A few additional things to check.

Check Application Security Prior to Development and Deployment

- Change Control - Stability, Assessment, and Testing
  - Has a proper impact analysis been performed related to the change?
  - Has the impact of the changes been reviewed by someone with sufficient knowledge and authority?

Check Application Security Prior to Development and Deployment

- Accountability and Segregation of Duties
  - Are system audit trails developed such that they can be traced back to approvals in the change control system?
  - Make sure the application does not create SoD issues.

Check Application Security Prior to Development and Deployment

- Access Control
  - Ensure role-based access control is in place
  - Define which job role has the authority to use and update the application
  - Ensure that the application does not allow access to other programs outside of the assigned business dept. (or architecture, such as direct access to the backend database)
  - Evaluate method and location of the authentication.

Check Application Security Prior to Development and Deployment

- Confidentiality
  - Data classification – Know how sensitive the data is and that the application is handling it according to policy and regulation.
  - Data transmission – Does the data cross security domains, networks, etc..
  - Data encryption – Ensure you use this where and when it is required.

Monitoring, Business Continuity, Disaster Recovery, and Incident Response

(Going beyond the obvious)

Monitoring Effects on BC, DR, and IR, and Audit and Compliance

- Business Continuity, Disaster Recovery, and Incident Response
  - Organize monitoring as the starting point for your BC, DR and IR processes
  - Monitoring is the center around which you can position BC, DR, IR, and ultimately Audit and Compliance
    - Detection of anomalies (IDS, IPS, AV, etc.)
    - Detection of outages or service delivery problems
    - Triggers responses – BC, DR, IR processes
- Can be adapted to accommodate daily, weekly, monthly, reporting and developed to provide more efficient auditing, compliance, and risk assessments.

Monitoring for Audit and Compliance

- Reduce the complexity of audits.
  - Don't run the auditors' scripts, use your own tools.
  - Have the auditors check the process and tools for control and effectiveness.
- Once you are in control of monitoring, use it as a tool to aid in audit and compliance by making it routine.
- Create periodic reports (e.g. monthly Risk Management Report, or User Access Rights Review reports) of at least the data required by policy. Keep it simple and relevant.
- Use these reports, along with all testing, self-audits, etc., as a basis for generating audit data.

How many of you are in charge of, or otherwise responsible for, security and risk management?

Friendly Advice for Information Security Officers and Risk Managers

A few random thoughts on Technology, Security, and Risk

- Executive Management doesn't care about security - They care about business risk.
- Security is a means to reduce risk. Approach it that way.
- CISO risk tolerance doesn't matter as much as Executive Management's (and/or BoD) risk tolerance. (CISOs take note of this)
  - As nervous as the CISO may be about an issue, their responsibility is to assess risk and communicate to Executive Mgt so they can make informed business decisions.
  - If a risk can't be mitigated or reduced, let them know about it, and then get some sleep. *(Until it gets exploited)*
- Risk Management is about reducing exposure.

A few more thoughts on Technology, Security, and Risk

- Security is not an experiment in anti-hacking or a playground for technology geeks. Those who want to play must either change or be terminated. The business and legal risks are too great to deal with childish behavior or ineffective security and risk management.
- Policy and security measures are usually bypassed for business reasons, or simply to get the job done – typically working towards legitimate business goals. Realize this and use education and realistic security controls and practices to manage risk.

Final thoughts on Technology, Security, and Risk

- When you are not in control, time & other resources are not effectively used. Executive Mgt sees this. Good luck on getting your next budget approved.
- Executive Mgt needs to make well informed decisions. Technology Risk Mgt. *(indeed the whole Info Sec Program)* needs to ensure that Mgt. can do that.
- Business planning is named that way because that's what it is. Justify your capital and operational expenditures in terms of business risk. Management understands risk – not security
- Stability is the foundation upon which you can build a successful security and risk management program.

Governance

and

Guidance

Providing both Governance and Guidance to the Rest of the Organization

- Guidance is sought more now than in the past.
- The rest of the organization needs to be able, and feel comfortable with, approaching TRM for guidance.
  - It helps raise awareness and involves the entire team
- Success is achieved by clearly defined roles and responsibilities throughout the organization.
  - If everyone understands their role and how it affects each business area, risk and governance are simplified.
  - It is important that security not over-step into the business area.
    - It is our responsibility to provide due care, analysis and disclosure of security risks.
    - It is up to the business to decide whether or not the risks are acceptable. Business/App owners must own the risk.

What is the most significant strategic change you can implement regarding Application Security?

What is the most significant strategic change you can implement regarding Application Security?

- Security reviews and risk assessment early in the SDLC.
- Integrate SDLC and Change Management – Which also involves others in the process.
- Segregation of Duties within IT.
- Effective and Auditable Access Control

Other helpful additions to your applications

- Add audit capability to your applications. Make audit routine.
  - Especially where access issues are always audited.
- Add in any other check, logging, monitoring, or other capability required by policy, regulatory compliance, or other legal obligation (e.g. Litigation on Hold)
  - Read the policies and know what the compliance objectives are.

Metrics

How Reporting Metrics Can Assist in Detecting Many Types of Risk Concerns

- There is difference between logging events and meaningful metrics.
- Metrics need a context in order to be meaningful.
  - Identify which metrics are most critical to business and IT risk management; and which metrics you need to retain for audit, compliance, investigation, etc.
  - Include the critical data in the periodic compliance report, retain the rest for audit and investigation.
  - Periodic reports can aid in detecting issues and allow you to correct them prior to audit or certification of compliance by external parties. (e.g. Monthly Risk Mgt. report)
  - Periodic reporting may be required by regulation to ensure protection of customer data.

Top Reporting Metrics Regarding Applications and Risk

- Confidentiality
  - Access and authorization – Monitor and review unauthorized access occurrence.
  - Conduct user access rights reviews for inappropriate access.
  - Review SoD issues in the processes or access provisioning.
- Integrity
  - Change Management
  - Business requests for change vs IT Requests for change
  - Failed Change Management Processes
  - Comparison of system changes to change management list
- Availability
  - Business Uptime
  - Business Recovery

Specific Advice for Application Developers, Risk Management, and Auditors

Application Risk Management Recommendations – Design & Acquisition

- Review your application design and workflow prior to development. Add these checks to your security review.
  - Classification of the data. Does sensitive information cross between security domains?
  - What is the method of authentication and where is the authentication being performed?
  - Will any data or user credentials be transmitted unencrypted across security domains or boundaries such as routers, networks, or firewalls?
  - Are all components supported within the organization, such as middleware, DB, OS, etc?
  - Clearly indicate who the business owner is. This person must approve and review all access and change, and owns the audit and compliance issues.
  - Use development frameworks such as OWASP and SAMM.
  - Identify all ports, services, and firewall or network changes in the design review. (Don't make me ask you for it later.)

Application Risk Management Recommendations – Access & Change Mgt.

- Define how access control will be implemented, monitored, reviewed, and audited in policy.
- Adapt your Change and Release Management processes to accommodate any unique needs of applications if necessary.
- Ensure there is an auditable process for each stage of the development lifecycle.
  - Review each application for changes to accessing data, systems, networks, etc.
  - Approvers must know and understand what objects they are approving access to.
  - Ensure Accountability
  - Ensure Adequate Segregation of Duties.

Application Risk Management Recommendations - Assessments

- Ensue that you perform vulnerability & risk assessments that include verifying policy compliance.
- Ensure that the process is clearly defined for resolving any findings prior to advancing code through the release process.
- Test your applications for security and stability.
- Ensure there are clearly defined processes for patches and updates to the application.
- Review the application several times for security, compliance, and stability before the release date.
- Ensure you keep an inventory of all supported OS, applications, databases, and middleware with versions.

Application Risk Management Recommendations – Audit & Compliance

- Include all audit and compliance requirements from your updated policies and standards in the application design and build.
- Include compliance and security checks in the Risk Assessment process.
- The final check prior to deployment should only be to verify that nothing has changed since the approved design and confirm it meets all security and compliance objectives. This should be done with enough time to resolve all of the issues.

Application Risk Management Recommendations – Exception Handling

- Establish clear processes for handling policy exceptions.
  - Exceptions should be rare, difficult to obtain, and they must be documented.
  - There should be a clear understanding who owns the audit and compliance issues for each exception.
  - Too many exceptions to policy indicates that your stated risk tolerance in policies is lower than Management's risk tolerance.

Conclusions

- The top risk concerns for applications are the same top concerns for audit and compliance – from a risk mgt & audit point of view.
- TRM/ISO/CISO should be an ally and needs to provide both guidance and governance.
- Don't alienate Internal Audit. You're all on the same team. Likewise for you auditors.
- Make auditing your applications routine. Incorporate audit and compliance in the policy; design, or acquisition, of applications.
- Use Monitoring as a core for BC, DR, IR, reporting, and audit.
- Situational Awareness of the entire organization is paramount.
- Think of stability as a business decision. Keep stability in mind as the key to efficiency, cost effectiveness, and security.
- Think of security and risk management as business decisions. Frame your presentations and budgets in a business risk context.

Additional Sources of Information

- Application Security, Frameworks, and Tools
  - OWASP http://owasp.org
- Stability, ITIL, High Performing IT
  - The Visible Ops Handbook http://www.itpi.org/home/visible_ops_books.php
- Security
  - The Visible Ops Security Handbook http://www.itpi.org/home/visible_ops_books.php
- For Policy Frameworks
  - Federal Financial Institution Examining Council (FFIEC) http://www.ffiec.gov
- For Change and Release Management
  - The IT Process Institute http://www.itpi.org

Questions?

Contact:
pperfetti@impactsecurityllc.com
http://impactsecurityllc.com