Agile Risk Management – 30 Practical IT Security Evaluation Methods for IT Governance & Audit Professionals

CJ Bordoloi, CEO, TopPatch

Governance, Risk & Compliance – G31

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

2013 Fall Conference – "Sail to Success"

CRISC

CGEIT

CISM

CISA

#1: APPLICATION WHITELISTING

#1: Application Whitelisting

Exclusive list of applications allowed to be installed/run on your network.

- Determine what applications your organization cannot live without for your whitelist.
- Prevent any other executables and software libraries from operating on your network.
- Update user permissions so they cannot change the files that can be executed. Practically, this means only one or two system administrators have whitelist edit rights.

Whitelisting is much more of a political challenge than a technical one.

- From a security standpoint, whitelisting is an upgrade to any blacklisting policy.
- From an end-user perspective, whitelisting can be seen as hampering user freedom and impacting productivity. Therefore, user education may be necessary.

#2: APPLICATION PATCHING

#2: Application Patching

Unpatched software provides one of the most prevalent attack vectors for workstations, servers, networks

- Vulnerability patching is the lifeblood of sustainable IT security
  - All software has weak elements in its code, which are essentially virtual security holes. Criminals break into your systems and networks by going through these holes.
  - When software companies find out about the vulnerabilities in their software, they build and send out fixes, or "patches," to cover those security holes.
  - This happens almost on a weekly basis for the most widely used software products.

- The beauty of "application patching" as a strategy specifically is that it:
  1. Has very little internal resistance
  2. Prevents intrusions and improves your security posture
  3. Highly increases security against malicious code execution

#3: OPERATING SYSTEM PATCHING

#3: Operating System Patching

One of the most cost-efficient, yet very effective, security strategies you can implement is making sure that critical security patches are applied to all versions of all operating systems being used at your company

- Like application patching, operating system patching deters criminals from infiltrating your systems and network.
  - The key difference, though, is that it usually costs less to do.

- The concern that systems administrators responsible for rolling out patches often have is that a critical security patch **might destabilize the operating system or critical applications that run on it**, resulting in downtime and user frustration, while they execute a rollback to the system state prior to applying the patch.
  - This issue can be avoided using innovative patch testing methods in a QA environment prior to rolling out the patch

#4: NON-PERSISTENT VIRTUALIZED TRUSTED OPERATING ENVIRONMENTS

#4: Non-Persistent Virtualized Trusted Operating Environments

- **Deploying non-persistent virtualized trusted operating environments may be simply explained as virtually partitioning areas of your IT infrastructure for separate tasks**

- Ex: Let's take a risky activity like browsing the internet, which is an easy way to get infected with malware.
  - In a non-persistent virtualized trusted operating environment, that risky activity would be conducted on the organization's internet gateway, which would be separated from private and case-sensitive information like financial or medical records.

- In essence, you are creating two areas on your network
  - One area that has a high risk of breach potential for performing but without getting valuable information stolen
  - One area for all tasks that require access to company confidential information

- However, despite having excellent overall effectiveness with a policy like this, there are generally high upfront costs and lots of user-resistance
  - In this case, every organization and environment is unique, you simply have to perform an ROI analysis to see if the cost is worth the reward

#5: HOST-BASED AND NETWORK-BASED INTRUSION DETECTION/PREVENTION SYSTEMS

#5: Host-Based and Network-Based Intrusion Detection/Prevention Systems

Host-based and network-based intrusion and detection systems should be a no-brainer as far as security goes.

- Simply put, these internal systems are designed to find and stop unusual activity on your desktop and network

For host-based systems, key problems to look out for are:

1. Process injection (inputting malicious code to alter the behavior of other programs)

2. Keystroke logging (malware that tracks your keystrokes which practically looks for usernames and passwords)

3. Driver loading (intruders installing false openings -- drivers -- to allow easy access into systems)

4. Call hooking (changing the behavior of operating systems or applications by intercepting function commands)

For network-based systems, signatures and heuristics are key because they can be used to identify unusual traffic both internally, and crossing network perimeter boundaries

#6: THE BASELINE STANDARD

#6: The Baseline Standard

Baselines are the minimum level of protection required per system type, which indicates the necessary settings and the level of protection being provided

- Using a baseline standard, you have a defined level of security for every system on your network.
  - This allows you to ask, "Is this system secure? Yes or no?" based on quantitative points.

There are three easy ways to sink below your baseline, which can all affect security if not properly tested:

1. New software is installed

2. Patches or upgrades are applied to existing software

3. Other changes to the system take place

Security personnel must use automated methods to assess systems for every change and compare it to the baseline level of security

#7: VULNERABILITY ANALYSIS

#7: Vulnerability Analysis

Vulnerability Analysis- It is when an organization scans their systems for all the security holes that a hacker can exploit

Examples of security holes that a vulnerability analysis Identifies:

1. Missing patches

2. Misconfigured settings

3. Orphaned user accounts

4. Program code mistakes

It is important to perform these scans on a quarterly basis.

- **Ex:** Think about it this way, you go to the doctor's office to get check-ups every year or so to make sure you are generally healthy-- especially for vital analysis, like blood-work, that you can't see yourself.
- It's the same idea with networks -- the best time to get a check-up is when you don't think anything is wrong. Then, you're either right, and you're set, or you have issues which you can fix before they become a problem

#8: COMMON AREAS FOR VULNERABILITIES

#8: Common Areas for Vulnerabilities

List of Top 6 Common Vulnerabilities:

1. A service running on a server

2. Unpatched applications or operating systems

3. An unrestricted wireless access point

4. An open port on a firewall

5. Minimal physical security that allows anyone to enter a server room

6. Unenforced unique password management on servers and workstations

Remember, finding and eliminating vulnerabilities isn't a 'once-and-done' action -- it is a process that needs to be repeated periodically

#9: RESTRICTING LOCAL AND DOMAIN ADMINISTRATOR PRIVILEGES

#9: Restricting Local and Domain Administrator Privileges

As much of a no-brainer as it may seem, some organizations simply do not restrict administrator privileges nearly as much as they should

- When too many people have the ability to make significant changes within a network, there is more opportunity for both external and internal threats to tamper with the security configuration of the network.
  - Also, it is a lot easier to find a username and password from a group of 30 than it is a group of 3

- In addition to only allowing a handful of people to have administrator privileges, it is a safe practice to restrict their email and web-browsing functions to be performed on a separate, unprivileged account to protect the privileged account from being infected by malware

#10: THE PURPOSE OF RISK MANAGEMENT

#10: The Purpose of Risk Management

- Since we have a finite amount of risk management capital, and an almost infinite number of vulnerabilities, **it is important that we properly rank the most critical vulnerabilities to:**
  1. Ensure that we are addressing the most critical issues
  2. Achieve the highest return on investment

- **Crowd-sourcing Risk Management**
  – Ex: Google is offering $3 Million in total prizes at its third annual Pwnium event-- a hacking competition in Vancouver-- to anyone who can demonstrate vulnerabilities in the Google Chrome OS operating system.

#11: USE DIFFERENT FORMS OF AUTHENTICATION

#11: Use Different Forms of Authentication

- **Multi-Factor-**Using many forms of authentication for a username and password is called
  - Why? What is the value of multi-factor?
  - Deters 'bots' or 'key-loggers' from taking your usernames and passwords, giving them to criminals, and accessing your private
- **General rule of thumb:** For each new level of privileged information, add another form of authentication
- Despite the high costs of implementing this kind of policy, it is an extremely effective preventative measure for avoiding security breaches

#12: FILTER INCOMING AND OUTGOING WEB CONTENT

#12: Filter Incoming and Outgoing Web Content

Filtering incoming and outgoing web-content should be high on your list of "Who wouldn't do this!"

For the filters themselves, you could use one, or a combination of, these tools:

1. Web-content whitelisting
2. Behavioral analysis
3. Reputation ratings
4. Heuristics
5. Signatures

Cost or user-resistance may be quite high based on the level of filtering you want to enforce but may well be worth it

#13: SPOOF EMAIL BLOCKING

#13: Spoof Email Blocking

- **"Spoof Email"-** When a sender changes his or her email address and email heading to appear as if it is coming from a different-- usually trusted– source
  - Email spoofing is a way for criminals to impersonate your friends so they can easily break into your system
- Two examples of tactics to prevent against this form of attack are:
  1. Implement anti-spoofing policies, procedures and tools that enforce the rules e.g. Sender ID
  2. Create a Sender Policy Framework (SPF) record, and customize the settings to "hard fail"
- **SPF-** An email validation system that checks sender IP addresses
  - Administrators can then make SPF lists, or 'records,' of all the trusted domains.
  - When you customize your setting to "hard fail," it simply blocks everything not listed in your trusted domain list-- the SPF record
- As with all security configurations, both of the above tactics have their own pros and cons
  - You have to decide what is right for you organizations

#14: CENTRALIZED AND TIME-SYNCHRONIZED

#14: Centralized and Time-Synchronized

- **Logging-** recording changes on a network
  - **'Centralized'** and **'Time-synchronized**' logging = having one central server which logs system characteristics at specific intervals

- Key changes that you should definitely log with this method are:
  1. Successful and unsuccessful events
  2. Allowed and blocked network activity

- Then, analyze your logs for abnormalities
  - It is important to store your logs for at least 18 months or longer, especially for compliance audits

#15: CORRECT ANTI-VIRUS CONFIGURATION

#15: Correct Anti-Virus Configuration

Tips to make sure your anti-virus software is actually doing its job:

1. **Update regularly** -- new viruses are constantly developed to circumvent existing software, so make sure to at-least update your antivirus when your computer reminds you
   - Most antivirus software now also has an automatic update feature, so as long as you click that setting, you don't even have to think about it

2. Specifically, make sure your **software has up to date signatures, reputation ratings and other heuristic detection capabilities**

3. **Diversify the vendors you use for antivirus protection**
   - That way, criminals have a more difficult time infiltrating your systems because there isn't one easy breach mechanism to break into every system

#16: EDUCATE USERS ABOUT PASSWORDS

#16: Educate Users About Passwords

How many of your users use either their addresses or telephone numbers as part of your password phrases?

- Here are the key attributes of a strong password policy education for users:
  1. Complexity (different letters, capital and lowercase letters, numbers, and special characters)
  2. Lengthy pass-phrases that can be remembered easily e.g. "I l0ve l0llip0ps!"
  3. Avoid repeatedly using one password for multiple systems. Users should be advised to have at least one pass-phrase each for online banking, personal e-mail, online shopping and
  4. Avoid exact dictionary words

#17: THE TROJAN HORSE OF IT SECURITY

#17: The Trojan Horse of IT Security

How can your network still get compromised if it is secured, all antivirus and firewalls are properly configured, all software is up-to-date, and company security policies are enforced strongly?

- Of the many ways a criminal can circumvent the security protection, one is to utilize an unsuspecting user to open up an access gateway

- A criminal can infect an employee's removable and portable media device -- USB flash drives, portable hard-drives, mp3 players, etc.-- at an offsite location like the home with substantially less security
  - Once that employee inserts that device into their company's workstation, the employee just did what the criminal needed -- infiltrated the network with the right malware to secure root access

- One way to protect a network internally is to implement these key aspects of a Data Loss Prevention:
  1. Secure storage
  2. Rule-based handling
  3. Whitelisting certain USB devices
  4. Encryption
  5. Destruction

#18: TRANSPORT LAYER SECURITY

#18: Transport Layer Security

- **Transport Layer Security (TLS)-**used to prevent legitimate emails from being intercepted and reused for social engineering
- It is common for cyber-criminals to try and infiltrate a network by designing an email that looks identical to a friend or colleague's email, so the receiver will open the email and have the malware infect the workstation
- TLS encryption makes it much more difficult for those criminals to be able to recreate an email because they won't know exactly how to make it look
- Practically, you want to use TLS encryption between email servers and perform content scanning after the email traffic is decrypted

#19: MANAGE CONFIGURATIONS

#19: Manage Configurations

Control as much as you can control to make your life as simple as possible.

- In security, a good, low-cost strategy to help protect your IT environment is to manage computer configurations based on a hardened **Standard Operating Environment**

- **Standard Operating Environment-** every workstation on the network has the same operating system and software.
  - **Benefit-** There is a reduction in the cost and time to deploy, configure, maintain, support, and also, for security purposes, manage computers.

- It is imperative that for your Standard Operating Environment, you disable unrequired system functionality
  - Examples of this include IPv6 and autorun (the Windows based component to install new hardware and software)

#20: MALWARE EXPLAINED

#20: Malware Explained

- Malicious software or **'malware'** is a blanket term for a variety of different forms of computer code which can infect a system.
  - Examples include computer viruses, ransomware, worms, trojan horses, rootkits, keyloggers, dialers, spyware, adware, malicious BHOs, and rogue security software
- The objective of malware is to steal confidential information from systems and then move on to another target and repeat.
- Malware targets end-users through a variety of different means such as e-mail attachments, websites, penetrating cloud infrastructure, and mobile devices.
- Generally, today's 'modern day malware' focuses on fooling system security by avoiding signature and behavioral detection.
- Also, the current malware looks to disable antivirus software.

#21: WHAT CYBER-CRIMINALS ARE LOOKING FOR

#21: What Cyber-Criminals Are Looking For

Common 'not-so-intuitive' ways that criminals are exploiting unpatched software:

1. **New hardware:** Criminals are now constantly scanning address spaces of their targets--they are looking for new hardware to be attached to the network.
   - The reason for this is that new hardware generally doesn't come with the most up-to-date software, so essentially there is a small window of hardware vulnerability from when it gets installed on the network, and when it is given proper patches

2. **Portable devices like laptops:** Since laptops are not always on the company's network, they also aren't always patched with the same frequency as any other system on a network

- Because of that infrequency, criminals are also looking for those portable laptops to exploit

A common practice for criminals who are looking to exploit a network by one of these means is to attack at night.

- Hardware is generally installed at night and not patched until the morning, so that window gives intruders the time they need to install backdoors on those new systems

Easy Fix to this- Once you install anything new, automatically update it

#22: HARDENING WIRELESS SECURITY

#22: Hardening Wireless Security

To get around physical security and firewall protection, cyber-criminals try to enter networks through wireless access points within an organization

Here are 3 quick ways of protecting your organization from an unknown wireless attack:

1.Keep track of every device on a wireless network.

- Deny access to any device without an authorized configuration and profile defined by a standard company security policy

2. Use specific enterprise management tools to control all the wireless access points on a network

- Make sure to not use access points for the home because generally they do not allow for this kind of specific enterprise management capabilities.

3. All wireless access points should be detected by network vulnerability scanners. Therefore, you are able to see what access points are legitimate and have the ability to shut-down any unauthorized point.

- Further, employees who take their portable computers or laptops off-site and log on to the internet (taking your work laptop and checking your email at a coffee shop for example) are easily exploitable because of the drastically diminished internet security.
  - Criminals then use those exploited machines as a back door once the device is reconnected to the company's network

#23: FIREWALL EXCEPTIONS

#23: Firewall Exceptions

- As users demand exceptions to firewall protections over time for various projects and business needs, those exceptions often weaken the overall security of the network because the exceptions are not tracked and forgotten about after the completion of the project
  - Criminals know about these kinds of ‘exception’ policies and results, so they constantly search for security holes in firewalls, routers, and switches
  - By exploiting these flaws for this kind of circumstance, the criminal has the opportunity to redirect network traffic to a malicious system posing as a trusted system. In this process, the criminal can gain access to private data, and alter information

Here are 2 simple fixes to improving security over time:

1. Using the standard defined configurations in an organization’s security policy, compare all current firewall, router, and switch configurations

2. Implement ingress and egress filtering for interconnection points for specific ports within a network and only use those ports for these business needs exceptions.
   - This way, a network only allows the exception vulnerability in a segmented portion of the network, so if there is a compromise, it will not be able to spread to more crucial areas of the network

#24: STRONG NETWORK ARCHITECTURE

#24: Strong Network Architecture

- You can have all of the correct firewalls, antivirus, and security policies in place, **but all of that time, money, and energy will be in vain if you do not have a carefully implemented network architecture with security in mind.**

- Criminals can easily scan networks for vulnerabilities and can tell with relative ease when a network has simply evolved over time based on need rather than careful thought to security
  - This form of scanning is called **'mapping a network'**
    - It allows criminals to maneuver efficiently to access target machines.
    - They look for unnecessary connections between systems, improper filtering, and little to no network separation.
    - In other words, they are trying to find common weaknesses paramount to a weak network architecture.

- If you want to implement strong network architecture, the foundational principles are actually quite simple--think about it this way-- the more layers of protection you have, the more strong your architecture is.

- **The rule of thumb -** You want to **implement at least a 'three-tier architecture' policy** using a DMZ, middleware, and private network-- essentially, you mandate specific parts of your network be used for specific tasks.
  - For example, you may choose to mandate that the DMZ portion be used for any system accessible by the internet, but never used for sensitive data.

#25: THE IMPORTANCE OF DATA RECOVERY

#25: The Importance of Data Recovery

- When criminals enter a network and compromise machines, they tend to make changes to system and software configurations
  - They may also make more subtle changes to actual data on networks which ultimately jeopardizes organizational effectiveness
- If the criminal is able to execute these types of attacks, it becomes very difficult for an organization to repair all of the damages if there is no efficient data recovery process in place

Here are three basic steps of a data recovery program:

1. Backup all files, operating systems, and application software at least weekly. You should backup more frequently based on the importance of the data.

2. Constantly test backup media by performing a data restoration process. This ensures that the backup is properly working.

3. Train key personnel on both the backup and restoration processes so if there is an attack, data will be restored as quickly as possible.

#26: IMPOSTER USER ACCOUNTS

#26: Imposter User Accounts

Does your company hire sub-contractors on a temporary basis? Has an employee ever left your company for any purpose?

- If so, your company is susceptible to criminals finding those former employees' user accounts before they are deactivated, and taking them over to conduct an attack
  - Basically, they take legitimate, former accounts, and pass them off as current and active

Here are some quick ways of preventing this kind of cyber-intrusion:

1. Cross check all user accounts with business processes and owners. If an account cannot be associated with one, then eliminate it immediately

2. Create an expiration date for each account and move that date back periodically if the person/people are still with the company

3. In your official security policies, make a point of revoking system access immediately after the termination of an employee or subcontractor

4. Generally monitor all accounts and have a set time-frame for logging off users if they are inactive

5. If an account has not been used for a certain amount of days, notify the user of their inactivity. If there is still no activity, disable the account

Examples and solutions like these may seem simple, but often time the simplest fixes, mean a world of difference for an organization-- at an extremely small price too!

#27: INCIDENT RESPONSE

#27: Incident Response

The only true way to mitigate cyber-crime from affecting your network is to disconnect it all internet access points, but we all know that business productivity and user satisfaction will be greatly impacted if we do that

Because security is always a chess match between the criminal and the defender, inevitably there will be breaches, and therefore, **we must prepare for those breaches**

All formidable incidents will have these four elements:

1. Detection

2. Containment

3. Eradication

4. Recovery

Without all of these pieces, a criminal will have the ability to damage a network (and your organization's brand image) much more critically in a repetitive manner

#28: ROI CONSIDERATIONS FOR SECURITY MANAGEMENT

#28: ROI Considerations for Security Management

- **Cyber-security is similar to the insurance industry in some ways:**
  - You have critical (and not so critical) assets to secure, and you use antivirus, firewalls, and a whole suite of other security measures and applications to do so, just as folks do in the insurance industry to manage various risks
  - **However, despite the monthly or annual costs, there actually is a reasonable return on investment for the spend on hardware, software, people and processes**
- **To put it simply, you don't want to spend more money securing an asset that isn't worth at least equal to the amount of money it takes to secure**
  - For example, if you purchase a $1000 LED TV, you are not going to put a $100,000 insurance policy on it.
  - **The same idea holds true for internal information**
- **Pay special attention to personnel productivity costs**
  - Like any other department, you want to have maximum efficiency with each IT security employee to maximize your investment in their salary
  - By initially spending more for easier-to-use and efficient products, team members will be able to devote more time to their most important projects, and generally have less aggravation if a particular product is inefficient and creates more work for them

#29: PHYSICAL SECURITY

#29: Physical Security

- **You must physically protect the actual hardware (your servers) that contain your valuable information assets**
  - You can spend millions of dollars on firewalls, antivirus, monitoring, patch management, logging, authentication, and a plethora of other security items, but if a criminal is clever, and most are, and they see your servers with their own eyes in an unlocked room with nobody looking, well voila! That criminal just walked off with your server that contains your entire company's financial records!

- Like all other forms of security, there are certain levels of protection you can choose to implement based on how critical your assets are
  - For example, server rooms should be locked from the public--how many locks and what kinds are up to you based on how much money you are willing to spend.
  - You can put the servers themselves in a locked cage, so even if an intruder gains access to the room, it will be very difficult to remove the server without a key

- Next, your server room should not have windows where any outside observer can see the servers and access the room without resistance
  - You can even have a security guard stationed outside of your server room to ensure that no intruder enters.

By having these forms of preventative measures in place, you successfully mitigated a 'no brainer,' yet extremely important vulnerability

#30: EDUCATE YOURSELF!

#30: Educate yourself!

- **In a quickly changing and evolving technology industry, it is imperative to educate yourself with current trends to keep your organization secure**
  - Just as a doctor goes to med school and gets their degree, but also stays current with medical journals and modern day health issues, security professionals bear the same responsibility

Here are some common areas that any organization can focus on:

1. Evolving internet threats

2. New types of spear phishing socially engineered emails

3. Weak passphrases

4. Passphrase reuse

5. Unapproved USB devices

Remember, these points of security for any user are best practices for today. Constantly read the news and ask professionals in the industry to stay up-to-date. You never know when the simplest fix can be the difference between a dream and a nightmare