IARIA 2021 Tutorial 4

Disaster Recovery Plan, Management Response Framework and Penetration Testing

Dr Bob Duncan

April 18 – 22, 2021

Dr Bob Duncan

30 years in industry as a corporate accountant

6 years as a lecturer at University of Aberdeen

Research area cloud security and corporate compliance

Teaching Areas:

Computer Science

Cyber Security

Petroleum Data Management

UNIVERSITY OF ABERDEEN

Tutorial 2

Outline of Tutorial

Why these are important

Disaster Recovery Plan

Management Response Framework

Penetration Testing

Why these are important

- It is a matter of fact that your business will be at the receiving end of continuous cybersecurity attacks
- Unless you are extremely well prepared, one or more of these attacks will be successful
- Even if you are well prepared, it is likely that one or more attacks will succeed
- The difference in terms of what happens next depends on your level of preparedness

Why these are important (Cont.)

- The first thing you need to have is a solid disaster recovery plan, because once the inevitable happens, you do not want the whole company to be running around like headless chickens
- A well thought through disaster recovery plan that has been developed in detail, updated and regularly tested will be invaluable
- Everyone will know exactly what they have to do
- Actions will happen with organised efficiency

Why these are important (Cont.)

- A Management Response Framework is also another good tool to have at your disposal
- At times of crisis, a rapid, well thought out management response will be vital to recovering quickly and effectively
- If you leave it until that day dawns before you ask management what to do, you are already too late
- Whereas, if everything is already thought out in good time, there will be no mystery. Everyone will know exactly what to do

Why these are important (Cont.)

- How can we be sure our systems are secure and safe against attack?
- The best form of defence is to attack yourself!
- If you do not know all the weaknesses and vulnerabilities in your system, you can be sure attackers will find them quickly enough
- We resolve this by carrying out penetration testing against our own company
- Once we recognize all the weaknesses, we can fix or mitigate them

Disaster Recovery Plan

Outline of Disaster Recovery Plan

Prerequisites

Conventional Disasters

Information Technology Disasters

Preparation

Disaster Recovery Plan

Management Recovery

Disaster Recovery Plan

Prerequisites

- You need to understand all about the structure of the business architecture of the company you are going to work for
- If this has not been documented before your arrival, this will be one of the most urgent tasks that will be necessary for you to undertake
- If you do not understand this and a serious breach arises, then you too will end up running around like a headless chicken

Disaster Recovery Plan (Cont.)

Prerequisites (Cont.)

- Why would this be so?
- If you have no idea of what the business architecture of the company is, how could you possibly know how to assist with the Disaster Recovery process?
- Thus, as a precautionary measure, should this not be known, you need to make it abundantly clear on being hired that this must be your urgent priority to limit any possible damage
- Until that has been carried out, the company will be vulnerable

Disaster Recovery Plan (Cont.)

Prerequisites (Cont.)

- Of course, this will not be the only vulnerability
- Understanding what the company's business architecture is will only give you a start to tackling the problem. It will not provide any solution
- This is because you need to have put some serious thought into how you should deal with such a scenario long before it actually arises
- Otherwise, it will be headless chicken time …

Disaster Recovery Plan (Cont.)

Conventional Disasters

- A well organized company will at least have a conventional disaster recovery plan in place
- Of course, it is possible that a young company might not, in which case you should bring this matter to the attention of top management
- On the next page, we will look at the typical conventional disasters that are taken into consideration, and why this usually leaves IT rather short

Disaster Recovery Plan (Cont.)

Conventional Disasters (Cont.)

- In 2020, there were a total of 416 global natural disaster events, including earthquakes, tsunamis, tropical cyclones, wildfires, excess heat, drought, hurricanes, landslides, floods and volcanic eruptions
- These are major events, and the impact can be catastrophic on any business, including the impact on IT systems
- While it would be prudent to ensure these matters are taken into account, we should note that these events typically only account for some 6% of IT disasters

Disaster Recovery Plan (Cont.)

Conventional Disasters (Cont.)

- In the event that a conventional disaster recovery plan (CDRP) exists, it will likely form a sub-set of the Business Continuity Plan (BCP), which any prudent business will have put in place to ensure everyone knows what to do to get the business up and running again as quickly as possible
- Let us assume the BCP and CDRP are already in existence. There is a high likelihood that all of the above possible events will have been considered and mitigated for
- However, there is a high probability that a proper IT disaster recovery plan may not be in place, or may not address all the possible risks that the business could be exposed to

Disaster Recovery Plan (Cont.)

Information Technology Disasters

- So what could possibly be missing?
- What about human error, hardware and software failure, cyberattacks?
- These can all have a devastating impact on the business architecture of the company, leading to an IT disaster
- During the past three years, it is estimated that up to 93% of business have suffered a natural or man-made disaster – and many of these organisations were unable to recover

Disaster Recovery Plan (Cont.)

Information Technology Disasters (Cont.)

- Whether your company is large or small, the only way to prepare for any disaster is to develop and exercise a disaster recovery plan
- Thus we need to examine these potential areas more closely to understand what could possibly go wrong
- We will start by examining what exactly is an IT disaster recovery plan

Disaster Recovery Plan (Cont.)

IT Disaster Recovery Plan

- An IT Disaster Recovery Plan (ITDRP) is a written document. It spells out the policies, the step-by-step procedures and responsibilities to recover an organisation's IT system and data. It also addresses getting IT operations back up and running as soon as possible after a disaster happens
- This plan needs to fit in with the conventional disaster recovery plan, since recovery from a natural disaster for IT systems may differ from the approach required for a human-caused IT disaster

Disaster Recovery Plan (Cont.)

IT Disaster Recovery Plan (Cont.)

- As an example, if a building is immersed in water due to a massive flood, destroying all the IT equipment, purchasing new IT equipment to run in that same location would not work. Clearly the premises would not be able to be re-used for a considerable period of time
- Thus the IT disaster recovery plan needs to relate precisely to an entirely different set of circumstances, which will require an entirely different approach will be required
- We will now take a look at what might be required

Disaster Recovery Plan (Cont.)

IT Disaster Recovery Plan (Cont.)

- First, let us consider the types of disaster we might encounter
- Human error could lead to a mass of data, or corruption of data, or data full of errors. A critical server might suffer a catastrophic failure. Important software could suffer a failure, sometimes due to a faulty update, with devastating consequences
- Of course, there is always the high likelihood of a cyber attack. Criminals are constantly trying to penetrate corporate systems to see what they might be able to steal, or possibly to cause maximum disruption of that is their goal
- Corporate IT systems are under constant attack from a wide variety of actors

Disaster Recovery Plan (Cont.)

IT Disaster Recovery Plan (Cont.)

There are many different types to consider:

- State actors
- Industrial espionage
- Hacktivists
- Organised crime
- Script kiddies
- Casual criminals
- Internal threats
- Employee carelessness

Disaster Recovery Plan (Cont.)

IT Disaster Recovery Plan (Cont.)

State actors:

- Exceptional skill set
- Extremely well resourced
- Often just want to see what the company is up to
- Skilled enough to get in and out of the system any time they like without your knowledge
- Sometimes they may be looking to acquire Intellectual Property
- Sometimes their goal is to cause disruption

Disaster Recovery Plan (Cont.)

IT Disaster Recovery Plan (Cont.)

Industrial espionage:

- Usually very skilled
- Well resourced
- Looking for Intellectual Property
- Highly motivated – sale of Intellectual Property is big business
- It will be hard to detect they have been in your system, at least until the competition brings out a cheaper version of your IP

Disaster Recovery Plan (Cont.)

IT Disaster Recovery Plan (Cont.)

Hacktivists:

- Often highly skilled
- Usually not well resourced
- Exceptionally motivated
- Looking to cause maximum embarrassment for the cause
- May cause disruption, deface web sites, delete data and so on

Disaster Recovery Plan (Cont.)

IT Disaster Recovery Plan (Cont.)

Organised crime:

- Usually use highly skilled people to attack you
- Very well resourced
- Looking for money
- Looking for data
- Looking for Intellectual Property
- Looking for ransom – perhaps by encryption your systems
- No moral scruples

Disaster Recovery Plan (Cont.)

IT Disaster Recovery Plan (Cont.)

Script kiddies:

- Often amateurs, which can lead to unexpected damage
- Some are very smart
- Frequently looking for the ‘kudos’ of being able to break in to your IT systems
- Often not looking to cause problems intentionally
- Not usually looking to steal money or data
- However, their lack of understanding and training can lead to unexpected damage

Disaster Recovery Plan (Cont.)

IT Disaster Recovery Plan (Cont.)

Casual criminals:

- Often very amateur
- May have bought hacking kits from the dark web
- Looking for whatever they can get
- Lack of knowledge can lead to unexpected damage to IT systems

Disaster Recovery Plan (Cont.)

IT Disaster Recovery Plan (Cont.)

Internal threats:

- Present a very serious threat
- They understand how internal systems work
- They may have high access levels
- They may understand how defensive systems work and may be able to circumvent them
- They may be out for revenge due to perceived ‘slights’ such as did not get expected promotion
- They may be in the pay of outside parties
- They could be seeking to steal money

Disaster Recovery Plan (Cont.)

IT Disaster Recovery Plan (Cont.)

Employee carelessness:

- Many employees do not understand how carelessness or errors can cause serious disruption, or even damage, to corporate IT systems
- Can be difficult to detect
- Sometimes the taking of shortcuts can undermine security measure in place

Disaster Recovery Plan (Cont.)

IT Disaster Recovery Plan (Cont.)

- We can see that there are indeed a great many challenges that are faced in trying to safeguard IT systems, and every one of these needs to be addressed
- How are we to go about this then?
- Depending on our system architecture, we can categorise the types of disaster recovery plans that we can utilise:
  - Virtualised Disaster Recovery Plans
  - Network Disaster Recovery Plans
  - Cloud Disaster Recovery Plans
  - Data Centre Disaster Recovery Plans

Disaster Recovery Plan (Cont.)

IT Disaster Recovery Plan (Cont.)

Virtualised Disaster Recovery Plans:

- You create a replica of the entire IT infrastructure and store this on an offsite Virtual Machine (VM)
- VMs are hardware independent, so you can easy restore data from your original systems
- When a disaster arises, you can failover IT operations to the offsite VM and recover from a disaster in a few minutes

Disaster Recovery Plan (Cont.)

IT Disaster Recovery Plan (Cont.)

Network Disaster Recovery Plans:

- A network disaster recovery plan helps your IT team respond to an unplanned interruption of network systems during a disaster
- The plan must address recovery of both LANs and WANs
- The interruption can range from performance degradation to a complete outage

Disaster Recovery Plan (Cont.)

IT Disaster Recovery Plan (Cont.)

Cloud Disaster Recovery Plans:

- With this type of disaster recovery plan, the entire system and data are backed up to a public cloud at least 150 miles away from the main site
- When a disaster happens, the IT can easily failover all operations to the secondary site and later fallback to the same or new hardware
- Since the cloud can be setup on pay-as-you-go basis, it can provide very cheap insurance in the event of an unexpected disaster

Disaster Recovery Plan (Cont.)

IT Disaster Recovery Plan (Cont.)

Data Centre Disaster Recovery Plans:

- This requires your company to set up a separate facility that is only ever used when a disaster happens
- There are three types of data centre disaster recovery plans – cold, warm and hot

Disaster Recovery Plan (Cont.)

IT Disaster Recovery Plan (Cont.)

Data Centre Disaster Recovery Plans (Cont.):

- A Cold Disaster Recovery Site is an office or data centre located away from the main site. It has power, heat, air conditioning and so on, but no running IT systems. These can be started up when a disaster arises, meaning some time delay and potential loss of data
- A Warm Disaster Recovery Site offers everything a cold site offers, but backups are done daily. There may be some minimal data loss
- A Hot Disaster Recovery Site offers everything a warm site offers, but in this case, everything is up to the minute up to date, meaning there will be no data loss

Disaster Recovery Plan (Cont.)

IT Disaster Recovery Plan Setup

Every business needs a disaster recovery plan that is tailored to its own data requirements. You need to understand the value of your data, systems and applications against the risk your organisation is willing to assume. Here are the steps you need to consider:

1 Establish a planning group

2 Perform a risk assessment in which you should define acceptable Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs)

3 Prepare an inventory of IT assets

4 Identify dependencies and establish priorities

Disaster Recovery Plan (Cont.)

IT Disaster Recovery Plan Setup (Cont.)

5 Develop recovery strategies

6 Develop a communications plan

7 Develop documentation, verification criteria, procedures and responsibilities

8 Test, test and test the plan again and again

9 Implement the plan

10 Maintain the IT infrastructure

Disaster Recovery Plan (Cont.)

What to do when a disaster happens

When the inevitable happens, it can cause chaos, which can lead to mistakes easily being made, even by your own team. It is a good ide for you to create your own list of Dos and Don’ts for plan development for use before, during and after the crisis

Let us start with the **Do Nots:**

- Do not discount the importance of an IT disaster recovery plan because you have backups or have implemented high availability. You need an IT disaster recovery plan **no matter what!**
- Do not consider disaster recovery an expense. It is **an investment**
- Do not apply a single data protection strategy to **all applications**
- Do not assume that your network can handle the traffic during an emergency. **Identify alternative forms of communication** if you cannot use the network

Do not create a disaster recovery plan **just for the sake of having one** or to simply satisfy executive management and your auditors

Disaster Recovery Plan (Cont.)

What to do when a disaster happens (Cont.)

Now for the **Dos:**

- Be sure to get sponsorship for the DR plan from the executive team
- Do look for disaster recovery plan examples to use as a template to speed the development and improve the accuracy of your plan
- Do include key contact members from various departments in your planning committee. Include decision-makers from a variety of departments as well as financial associates, customer service representatives, and IT personnel
- Safeguard data not stored centrally, including data stored on desktops, laptops, and mobile devices. Also consider the following:

Disaster Recovery Plan (Cont.)

What to do when a disaster happens (Cont.)

More **Dos:**

- Safeguard data not stored centrally, including data stored on desktops, laptops, and mobile devices. Also consider the following:

1. Virtual environments
2. Application-specific agents
3. Snapshot storage requirements
4. Server activation and documentation
5. Backup and recovery

Disaster Recovery Plan (Cont.)

What to do when a disaster happens (Cont.)

And even more **Dos:**

- Do create a disaster recovery plan checklist to use as a quick reference when developing the DR plan and during an actual disaster. A checklist helps your team work quickly and perform tasks accurately
- Do perform end-user acceptance testing
- Be sure to regularly test a broad range of disaster scenarios

Disaster Recovery Plan (Cont.)

What to do when a disaster happens (Cont.)

And finally even more **Dos:**

- Update and test your disaster recovery plan regularly
- Choose a disaster recovery location that is not too close to your production site and can be remotely activated in the event of an emergency
- Plan frequent meetings to ensure that resources are still available in the event of a disaster

Disaster Recovery Plan (Cont.)

A word about testing:

- It is **critical** that you test your disaster recovery plan to ensure you have all the elements in place for a successful test
- This should include a detailed script of test activities
- All IT components must be in place and ready to use
- Make sure you document what happens during the test
- Prepare a post Disaster Recovery test action review

Disaster Recovery Plan (Cont.)

And a word about your Disaster Recovery solution:

- Do not assume you will get it right on your first attempt
- Do not be afraid to suggest a third party provider if your systems are so complex that they are beyond the capabilities of the available teams
- Make sure you already have a solid backup solution already in place
- Without a solid backup strategy, your DR solution will be doomed to failure

Management Response Framework

Outline of Management Response Framework

Checking if you are Prepared

Classic Incident Management Frameworks

Modern Frameworks for the Age of Advanced Persistent Threats

Incident Management Maturity Models

Management Response Framework (Cont.)

Checking if you are Prepared:

- Some questions to answer:
- Did you create a disaster recovery team?
- Did you determine critical applications, documents and resources?
- Did you specify backup and off site storage procedures?
- Did you test and maintain the disaster recovery plan?

Management Response Framework (Cont.)

Checking if you are Prepared (Cont.):

What are the 7 tiers of disaster recovery?

- Tier 1 – No off-site data
- Tier 2 – Physical backup with a cold site
- Tier 3 – Physical backup with a hot site
- Tier 4 – Electronic vaulting
- Tier 5 – Point-in-time copies/active secondary site
- Tier 6 – Two-site commit/transaction integrity
- Tier 7 – Minimal to zero data loss

Management Response Framework (Cont.)

Checking if you are Prepared (Cont.):

Possible Key Elements of a Disaster Recovery Plan:

- Documentation ...
- Scope and Dependencies ...
- Responsible Team & Staff Training ...
- Secondary Location Configuration ...
- Setting the RPO and RTO ...
- Testing and Optimization ...
- Automation …

Management Response Framework (Cont.)

Checking if you are Prepared:

Here are 15 questions to help you with your design:

1 Identify Critical Business Processes

2 Label Dependencies

3 Define Vital Applications

4 Assess Your Current Data Recovery Strategy

5 Perform a Business Impact Analysis (BIA)

Management Response Framework (Cont.)

Checking if you are Prepared (Cont.):

6 Define Recovery Point Objectives (RPO)

7 Distinguish Recovery Time Objectives (RTO)

8 Designate Maximum Tolerable Downtime (MTD)

9 Assess Risks

10 Test Your Theory

Management Response Framework (Cont.)

Checking if you are Prepared (Cont.):

11 Redesign Accordingly

12 Implement New Solutions

13 Develop an Emergency Response Procedure

14 Align Procedure to meet DRP timelines and MTD Requirements

15 Form a Team

Management Response Framework (Cont.)

Checking if you are Prepared (Cont.):

Make sure to have covered:

- Recovery Point Objectives (RPO)
- Recovery Time Objectives (RTO)
- Remote Data Backup
- Accountability Chart
- DR Plan Testing

Management Response Framework (Cont.)

Common Disaster Recovery Plan Steps:

- Audit all of your IT resources
- Determine what is ‘mission-critical’
- Establish Roles and Responsibilities for everyone in the DR plan
- Set your recovery goals
- Consider a remote data storage solution
- Create a test for the recovery plan

Management Response Framework (Cont.)

Audit all of your IT resources:

- Before you plan for a return to ‘normal’, you need to understand what normal is in the first place
- Therefore be sure to audit **ALL** of your existing IT assets
- You need to understand where everything is within your systems architecture and what data each holds and processes
- This will help you understand how to start streamlining the whole process to ensure nothing is missed

Management Response Framework (Cont.)

Determine what is ‘mission-critical’:

- Your business probably stores far more data than you think it does
- But not all of it will be ‘mission-critical’
- By identifying what is vital from what may be unnecessary or redundant, it should be possible to reduce the amount of data required for the size of a recovery backup
- Take the opportunity to remove unnecessary data from endpoints where they are not needed

Management Response Framework (Cont.)

Establish Roles and Responsibilities for everyone in the DR plan:

- Every employee in the organization should have a role to play in your disaster recovery plan
- Something as simple as reporting cybersecurity threats up the chain of command can prove to be a critical aid to the success of the DR plan
- When everyone knows what to do in response to an emergency, your DR plan will be far more effective than it would be if nobody knew what to do when a disaster occurs

Management Response Framework (Cont.)

Set your recovery goals:

- You need to understand how quickly your company can recover from a disaster?
- How much and what type of data can you afford to lose?
- Setting goals for recovery point and recovery time objectives can prove to be a crucial part for making the DP plan effective
- Mission critical data should be prioritized, as should data that will be required right away
- You may even wish to use a Business Continuity (BC) plan for this data

Management Response Framework (Cont.)

Consider a remote data storage solution:

- If your business is hit by an attack that wipes out your main data server, that data could be lost forever
- Should your assets get physically damaged, the remote backup system could minimize business disruption
- The gold standard would be to use a cloud-based solution that could automatically download and keep data completely up to date
- There can still be a place for physical media backups which can help with data isolation to safeguard against a ransomware attack

Management Response Framework (Cont.)

Create a test for the recovery plan:

Make sure you have a means to test your plan to be sure it works:

- Check and address for single points of failure
- Check how long recovery time takes, as well as getting back to normal
- Check how much data could be lost when switching over
- Check all of this against different disaster types. Different disaster problems might require different solutions. Make sure you have a solution for each different disaster type

Management Response Framework (Cont.)

You now have plenty of advice about how to do this:

- We will also move on to look at a number of existing solutions that are available for specific requirements. You could use some of these as a guide to producing something suitable for your own company
- There are a number of classic incident management frameworks
- There are some modern frameworks for the age of advanced persistent threats
- And, of course, there are also some incident management maturity models

Management Response Framework (Cont.)

Classic Incident Management Frameworks

- There are a number of existing classic incident management frameworks available
- These are based on setting up the standard Computer Security Incident Response Team (CSIRT) approach, which can be used in companies, as well as at a higher national level
- Just be aware that these were developed before today's Advanced Persistent Threat (APT) style attacks started up, which means they are mostly based on the old linear method of Preparation, Identification, Containment, Eradication and Recovery model

Management Response Framework (Cont.)

Classic Incident Management Frameworks (Cont.)

- ISO/IEC 27035:2011 The Information Security Incident Management standard will provide you with a structured approach to detect, respond, report and learn from security incidents
- SANS Creating and Managing an Incident Response Team gives an overview of classic CSIRT activities and organisational requirements. A solid, easy to use, if rather outdated framework
- RFC2350 Expectations for Computer Security Incident Response is a standard produced by the Internet Engineering Task Force. It also provides a template for publishing the list of services and contact details for your own company CSIRT, for publication internally or externally

Management Response Framework (Cont.)

Classic Incident Management Frameworks (Cont.)

- CERT Handbook for Computer Security Incident Response Teams defines a governing policy framework around incident response and the list of services a CSIRT may provide. This also addresses quality assurance matters

- NIST 800-61 Computer Security Incident Handling Guide is produced by the National Institute of Standards and Technology of the US. The NIST framework lists necessary documentation of policies and incident response plans, as well as providing for typical information flows as well as defining the ideal lifecycle of incidents

Management Response Framework (Cont.)

Classic Incident Management Frameworks (Cont.)

- ENISA CSIRT Setting up Guide is a comprehensive EU model that addresses business, process and technology. It demonstrates the business value of having your own CSIRT. They also publish the ENISA Good Practice Guide for Incident Management

- ISACA Incident Management and Response – covers the ISACA approach to incident management based on Control Objectives for Information and Related Technology (COBIT) principles. It demonstrates the benefits of having an incident response team, defines the phases of the incident lifecycle, associated information security strategies and other governance activities. It also justifies having an IR function by linking it to the relevant COBIT function

Management Response Framework (Cont.)

Classic Incident Management Frameworks (Cont.)

- Providing you keep in mind that all of these classic options were developed before APT attacks came on the scene, there will be much useful information that you could learn from their content
- Of course, you will also need to adapt whatever you utilize to ensure you can meet the challenge brought by APT attacks

Management Response Framework (Cont.)

Modern Frameworks for the Age of Advanced Persistent Threats

- APT attacks involve highly targeted attacks such as AntiVirus Evasion, Powershell-based Backdoors and Advanced Beacons
- As a consequence, incident response practices are having to change rapidly
- At this time, may are still running hard to try and catch up
- ISACA Responding to Targeted Cyberattacks is another framework from ISACA, which takes a more practical approach to defending against APT activities. Developed in collaboration with Ernst & Young, standardises detection and response techniques
- Otherwise, this is a fast developing arena

Management Response Framework (Cont.)

Incident Management Maturity Models

- Here are some current Incident Maturity Maturity Models that can help your company measure their current maturity level
- SIM3 Security Incident Maturity Model that helps to assess the current level of capabilities of your Incident Response Team. It presents the next level and outlines the steps needed to achieve that
- CERT Incident Management Capability Metrics (IMCM) provides a comprehensive checklist based approach which can be used to assess how your current incident management capability is defined, managed, measured and can be improved

Management Response Framework (Cont.)

Incident Management Maturity Models

- CERT An Introduction to the Mission Risk Diagnostic for Incident Management Capabilities (MRD-IMC) is a method which uses a risk-based approach for assessing which incident management function achieves its mission and objectives

- The Threat Hunting Maturity Model is an ongoing activity where analysts actively scan the infrastructure of indicators for compromise. There are different levels of hunting from non0existent up to full automation

Penetration Testing

We will address Penetration Testing now

Penetration Testing (Cont.)

We can consider that there are three groups of people who are interested in Penetration Testing:

- Professional Penetration Testers
- In-house Defenders
- Attackers

Many of their interests and approaches are similar, but there can be subtle differences between their goals and requirements

Penetration Testing (Cont.)

Professional Penetration Testers:

- Professional penetration testers are frequently hired by corporates to test corporate IT systems to show how secure these systems are
- It is usual for them to be given a brief without details of what the corporate system architecture is
- The expectation is that they can carry out all their requirements without attracting the attention of the in-house IT teams
- In-house teams will not be informed that this will be happening

Penetration Testing (Cont.)

In-house Defenders:

- The in-house IT team assigned the responsibility for defending corporate systems should consider carrying out penetration testing of their systems to determine how vulnerable to attack it might be
- This can allow them to understand where improvements are required to increase the resilience of corporate systems to attack
- Without testing properly all corporate systems, it will be impossible for them to understand where weaknesses lie and how to strengthen them

Penetration Testing (Cont.)

Attackers:

- Often approach a company with no prior knowledge of how their business architecture is organized
- They need to find all of that information for themselves before they can realistically mount a serious attack on the system
- Many amateur attackers will simply dive straight in and attack systems without any advance knowledge or preparation, and these invariably result in failure
- The professional attackers are the ones to be concerned about

Penetration Testing (Cont.)

What does this mean for the corporate?

- All three groups will therefore seek to take a highly detailed and professional approach
- In this way, the professional penetration tester will be able to identify properly all the weaknesses in the system
- The in-house team will stand a better chance of defending the company
- The attacker will have a greater likelihood of succeeding with their attack on the company

Penetration Testing (Cont.)

Why should the corporate care?

- Having third-party professional penetration testers thoroughly test all aspects of corporate system can give the assurance that all known vulnerabilities have been addressed
- It should be obvious that by having a better understanding of vulnerabilities and risks, the in-house team will do a better job of defending corporate systems
- Attackers will not be seeking permission from the company to attack it, so corporates need to be aware that the attacks will come relentlessly, day in day out, and the better prepared they are, the lower the risk they face

Penetration Testing (Cont.)

How should a penetration test be carried out?

- For all three groups, the process will be remarkably similar, even if all the motivations are not necessarily the same in every case
- The process breaks down activities into distinct stages
- Each stage should follow on in a logical manner to maximise efficiency
- This way, each group will stand a greater chance of achieving their specific goals
- We will outline the approach next

Penetration Testing (Cont.)

Penetration test stages:

- Reconnoiter
- Mapping
- Discovery
- Exploitation
- Web Platform
- Mobile Applications
- Connected Devices - Internet of Things
- Infrastructure and Network
- Social Engineering

Penetration Testing (Cont.)

Reconnoiter:

- We search for open source information on the target
- Any useful information, such as IP addresses, domain and sub-domain names, types and versions of technologies
- Any technical information shared on forums or social networks
- Any data leaks
- Who the directors are
- Who important employees are
- Much of this information may not require us to access company systems at all

Penetration Testing (Cont.)

Mapping:

- Here we seek to list all functionalities of the target
- We seek better visibility of all critical and exposes elements
- This is particularly important if tests on all the functionalities are to be carried out as part of the penetration test
- For a large corporate, this stage will be very extensive
- Even small companies are likely to run a great many systems on their infrastructure these days
- The goal here is to be thorough and comprehensive
- This will involve direct investigation of corporate systems

Penetration Testing (Cont.)

Discovery:

- This is the start of the attacking phases
- Pentesters are looking for vulnerabilities across all systems
- A number of manual tests will be undertaken
- Also, automated tools will be deployed in this phase
- The goal here is to discover as many potential vulnerabilities as is possible across the whole company

Penetration Testing (Cont.)

Exploitation:

- In this stage, testing possible exploitations of the flaws identified in the previous stage takes place
- Attempts will be made to ‘pivot’ these flaws to see if further vulnerabilities can be exposed
- Full evaluation of potential vulnerabilities allows the establishment of their real impact on the company, which in turn demonstrates the criticality of each vulnerability

Penetration Testing (Cont.)

Web Platform:

- The web platform is the most recognizable access point for attackers
- Vulnerabilities in web server configuration and web applications need to be discovered and identified
- Open and insecure services need to be discovered (such as the OWASP top 10)
- Logical vulnerabilities related to workflow implementation must be found
- Any new discoveries concerning software used must also be found

Penetration Testing (Cont.)

Mobile Applications:

- Where a company uses mobile applications, these applications frequently have vulnerabilities
- Thus static and dynamic analysis of the application is needed, which might include reverse engineering tests
- Vulnerability tests while the application is running should be carried out
- OWASP also provides lists of common mobile vulnerabilities and these should also be tested for

Penetration Testing (Cont.)

Connected Devices - Internet of Things:

- IoT devices are traditionally one of the weakest links in the system
- The entire IoT ecosystem needs to be checked
- This will include hardware, embedded software, communications protocols, servers, web and mobile applications
- Tests on hardware, firmware and communications protocols would be specific to each device
- Such tests might include data dump via electronic components, firmware analysis, signal capture and analysis

Penetration Testing (Cont.)

Infrastructure and Network:

- These tests are performed on an external infrastructure and would cover the company's public Ips, services exposed online, service configuration and operating system architecture

- Tests on an internal corporate network would include mapping the network looking for vulnerabilities on workstations, servers, routers, bridges, proxies, printers and any other network devices in use

Penetration Testing (Cont.)

Infrastructure and Network:

- These tests are performed on an external infrastructure and would cover the company's public Ips, services exposed online, service configuration and operating system architecture

- Tests on an internal corporate network would include mapping the network looking for vulnerabilities on workstations, servers, routers, bridges, proxies, printers and any other network devices in use

Penetration Testing (Cont.)

Social Engineering:

- Often described as the ‘weakest link’, people in the company also need to be assessed
- Management need to understand how the reflexes of staff are when faced with phishing attempts, telephone attacks and even physical intrusion
- Sending of phishing and spear fishing emails, use of cloned interfaces, malware, collecting sensitive information via phone calls and malicious USB devices are just some examples of what might be done

Penetration Testing (Cont.)

What is the outcome of a penetration test?

- This depends on who is carrying it out
- For the professional penetration tester, a successful outcome will produce a very detailed report of potential weaknesses including recommendation for best practices to implement
- For the in-house defender, weaknesses and vulnerabilities are identified and hopefully can be mitigated or patched
- For the attacker, a successful outcome will be a good day at the office. Unfortunately, it will likely not end well for the corporate, with a possible breach, disruption, possible legislative and regulatory fines, loss of reputation, adverse impact on share price

Penetration Testing (Cont.)

What happens next?

- Again, this depends on who is carrying it out
- For the professional penetration tester, a satisfied client and on to the next job, perhaps with a recommendation for further work needed
- For the in-house defender, successful closing of many vulnerabilities, perhaps identification of staff training needed and potential bonus for a job well done
- For the attacker, if they are good enough, having hidden a trapdoor in the system, a well earned break followed by a possible return at a later time for another bite of the cherry. In the event of un unsuccessful penetration, on to the next job until they get lucky

Penetration Testing (Cont.)

Post Penetration Activities for the Corporate?

- Identify security improvements needed
- Identify staff training required
- Identify additional testing needed
- Have a post breach debrief in the event of a successful breach
- Ensure necessary changes and training are implemented
- Improve Disaster Recovery Plan if required
- Maintain improved vigilance on IT activities
- Ensure a full and proper backup regime is in place
- Ensure all forensic records are protected

Disaster Recovery Plan, Management Response Framework and Penetration Testing

The end

WARNING

Use your new skills wisely and do not use your attack skills without first obtaining written permission from your target, otherwise you will be committing a criminal offence which will render you liable to prosecution

UNIVERSITY OF ABERDEEN