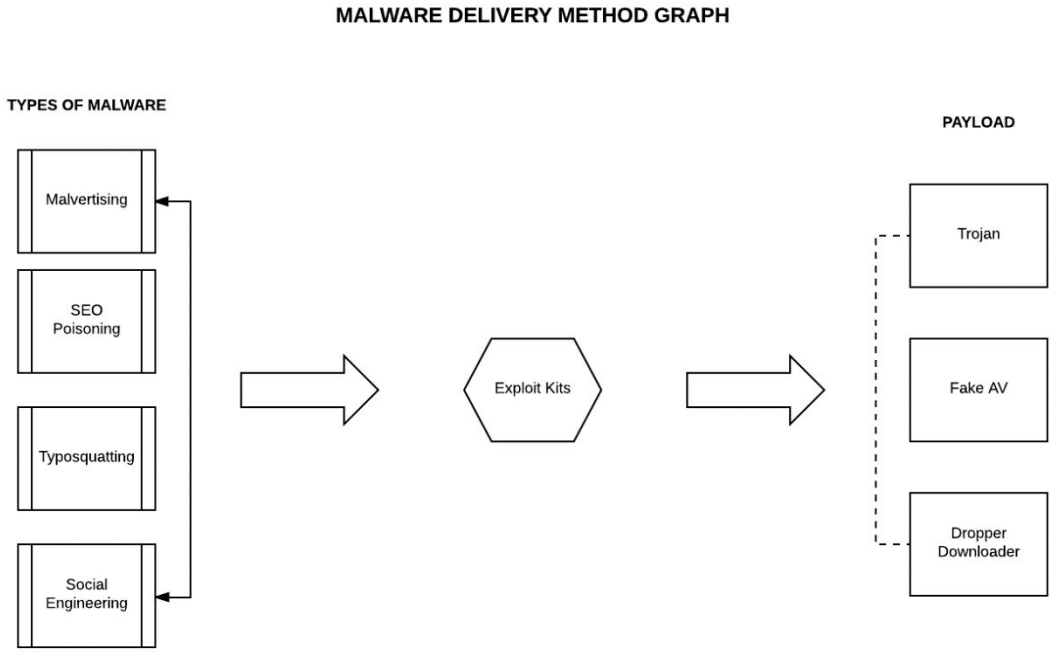
Omar

*** How people get affected**



Malvertising: Malicious ads displayed on websites leading to Exploit Kits.

SEO Poisoning: Malicious attackers inject common search terms in an iframe script designed to send victims to other sites hosting malicious code. The search term and iframe redirect and get cached in search engines such as Google. Victims who click on the links are sent to sites hosting malicious code.

Typosquatting: Also known as "URL hijacking," it is a form of cybersquatting which relies on typographical errors made by an internet user when typing a web address into a browser. If an incorrect website is entered, the user is led to a rogue website owned by a cybersquatter.

Social Engineering: Make use of URL shorteners, or social network like-jacking to disguise malicious links.

Exploit Kits: Drive-by downloads that can be activated simply by visiting a website with your browser. This is the most dangerous form of malware. No user interaction, or click, is needed to infect a user's computer.

Trojan: After installed on your system, this program will steal information to tunnel to outside parties (credentials, personally identifiable information (PII), espionage).

Fake AV: A rouge antivirus program designed to mislead people by posing as a legitimate antivirus program, but in reality it is only a fake version of the original software which gains access to a system with the help of bogus online scanners, insecure websites and Trojans.

Dropper Downloader: Downloads additional malware to an infected user's computer, without their knowledge or consent.

Types of malware

There are different types of malware that contain unique traits and characteristics. Malware, or malicious software, is any program or file that is harmful to a computer user. Malware includes computer viruses, worms, Trojan horses, and spyware. These malicious programs can perform a variety of functions, including stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity without their permission. A **virus** is the most common type of

malware, and it's defined as a malicious program that can execute itself and spreads by infecting other programs or files. A **worm** is a type of malware that can self-replicate without a host program; worms typically spread without any human interaction or directives from the malware authors. A **Trojan** horse is a malicious program that is designed to appear as a legitimate program; once activated following installation, Trojans can execute their malicious functions. **Spyware** is a kind of malware that is designed to collect information and data on users and observe their activity without users' knowledge.

Other types of malware include functions or features designed for a specific purpose. **Ransomware**, for example, is designed to infect a user's system and encrypt the data. Cybercriminals then demand a ransom payment from the victim in exchange for decrypting the system's data. A **rootkit** is a type of malware designed to obtain administrator-level access to the victim's system. Once installed, the program gives threat actors root or privileged access to the system. A **backdoor virus** or **remote access Trojan (RAT)** is a malicious program that secretly creates a backdoor into an infected system that allows threat actors to remote access it without alerting the user or the system's security programs.

How malware infects people

Infections spread by malware writers and attackers exploiting unpatched security holes or vulnerabilities in older versions of popular software such as Adobe, Java, Windows Media Player and the Windows operating system itself. The software is one of the favorite targets of malware writers who continue to exploit coding and design aggressive vulnerabilities. Cybercriminals constantly devise innovative means to get malware onto your computer. The most common ways that malware, including viruses, worms, Trojans, and spyware, can be spread by exploiting application tools as email, the internet itself, outdated software, local area networks (LANs), instant messaging and peer-to-peer file sharing systems, pop-ups, computer storage media and mobile devices.

Emails allow cybercriminals include malicious attachments and links in emails that appear to come from friends, reputable organizations, or other trusted sources. Some malicious emails can even infect your computer from the email client’s preview pane, without your opening or download an attachment or a link. **The Internet** allows for surfing the Web, which may feel like a private activity, but in fact, you’re exposing your computer to unwanted contact with anyone else who has a computer and Internet access. All you must do is visit a website or click a link and you’re a potential victim. Malware crawls the Internet, looking for vulnerabilities of outmoded software to spread its influence over computer systems. Be especially careful if you’re surfing the Web with **outdated software**. Make sure to never connect to the internet without being updated with the latest versions as soon as you can, including your browsers, operating systems, or system plug-ins. **Local Area Networks** (LANs) are a group of locally connected computers that can share information over a private network. If one computer becomes infected with malware, all other computers in the LAN may quickly become infected as

well. Also, if you're using a client for **Instant messaging** (IM) and **peer-to-peer (P2P) file-sharing** online systems activities, malware may spread to your computer. **Social networks** allow malware authors to take advantage of having the ability to infect the massive user-data networks with worms. If a social website account is infected with a worm, just about anyone who visits a poster's profile page could "catch" the worm on their system. Some of the most sophisticated malware spreads through well-disguised screen pop-ups that look like genuine alerts or messages. Malware can be easily spread if you **share computer storage media** with others, such as USB drives, DVDs, and CDs. While it may seem safe to open a CD of photos from a colleague, it's always best to scan unfamiliar files first for possible corruptions or security risks before you copy or open them. **Mobile malware** threats have become increasingly prevalent, as more people use their smartphones and tablets as mini-computers, helping malware problems proliferate across additional platforms. Malicious codes also spread into a system through **pirated software**. In the majority of the cases, software seems to be legitimate, when downloaded, instead, they are a be a big trouble for your system.

*** How malware affects people/businesses**

How malware works

Malicious programs **can be delivered physically** to a system through a USB drive or other means. Malware **often spreads via the internet** through drive-by downloads, which automatically download malicious programs to users' systems without their approval or knowledge. These are initiated when a user visits a malicious website. **Phishing attacks** are another common type of malware delivery; emails disguised as legitimate messages contain malicious links, or attachments that deliver the malware executable to unsuspecting users. Sophisticated malware attacks often feature the use of a command-and-control server that allows threat actors to communicate with the infected systems, download sensitive data and even remotely control the compromised device or server.

*** How malware affects the infected**

Malware is used for many different purposes, which is one of the reasons why it's so popular among cybercriminals. Malware can be used to:

- Hijack a user's session or computer
- Steal confidential data (like credit card info and SSNs)
- Compromise a website user's login information
- Make fraudulent purchases
- Launch DDoS attacks
- Create spam

Boost SEO rankings for a specific site, often a competitor's.

*** How businesses defend against malware**

Companies doe impose Security Controls to be a proactive defender of their proprietary processes and data they hold in their storage servers. **Controls (aka Countermeasure) are** actions, devices, procedures, or techniques that meet or oppose, counters, a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken. (NIST IR 7298 Revision 2, Glossary of Key Information Security Terms)

There are several types of controls that can be implemented in the design of the security processes within an organization. There are administrative, technical, physical controls that can be put in place to defend against any probable harm that can be imposed due to a company's naivety or negligence.\

Some sources, such as ISACA, draw a distinction between control and countermeasure. ISACA says a countermeasure is a targeted control. In this terminology, control is used at a strategic level, and a countermeasure is used at a tactical level. In practice in the corporate setting, the terms are used interchangeably.

TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

(NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations)

Security Controls: What to include in the Strategy
What Security Controls need to be included to have effective security protocols to resolve end-user folly?

Administrative security controls, or work practice controls, are technical, administrative safeguards or countermeasures that are changes in work procedures such as written policies, procedures, standards, guidelines, rules, supervision, schedules, and

training put in place to avoid, counteract or minimize loss or unavailability of data due to threats acting on vulnerabilities, such as a security risks. Controls are referenced all the time in security, but they are rarely defined. The purpose of this section is to define technical, administrative/personnel, preventative, detective, and corrective compensating controls, as well as general controls. **Technical controls** can be anything from a simple configuration change to a massive implementation. They tend to take a lot of time and resources are expensive. Technical controls are security controls that the computer system executes. The controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The implementation of technical controls, however, always requires significant operational considerations, and should be consistent with the management of security within the organization. Also, it should be known that it causes the biggest source of "security decay" issues. **Personnel controls** do ensure trustworthiness and integrity of employees. Makes it so that its more likely employees are experienced, honest and hardworking. It builds on natural tendencies to control or motivate the employee. Personal controls help clarify expectations of the employee, ensure each employee can do a good job, they increase the probability of self-monitoring and mitigate insider abuse. You need to be aware of legal issues especially in other countries when conducting **background checks. Organizations need to make** employees aware of standards, monitoring, and consequences. Also, companies need to invest in the heavy involvement of the HR and Legal departments. **Organizational structure** is a system used to define a hierarchy within an organization. It identifies each job, its function and where it reports to within the organization. This structure is developed to establish how an organization operates and assists an organization in obtaining its goals to allow for future growth. The structure is illustrated using an organizational chart. Organizational structure has effective reporting structures, as an example, the CISO reports to CIO, CEO, etc. There are clear lines of authority which tend to be either centralized or decentralized. **Centralized** gives more control to the CISO and more consistency, but may be unworkable in large and/or multination organizations. The d**ecentralized organization structure** is more flexible and puts local security staff closer to users but quality varies by location and visibility into issues are reduced. Recent high-profile incidents indicate the need for security awareness and training. In a world where employees are frequently exposed to sophisticated attacks, end-users can be the weakest link in the security chain. By bringing **education and awareness** to current incidents, organizations can be better protected from attacks by training technical and non-technical users alike. Education is required by many compliance regimes. Humans will almost always be the weakest link. End-users are also important in detecting incidents. Compliance with administrative controls requires understanding. Therefore, education must be ongoing. Organizations need to have realistic expectations of outcomes from awareness security protocol.

A computer **security audit** is a manual or systematic measurable technical assessment of a system or application. **Audits n**eed to be conducted internally and externally. Often, audits are usually conducted under the direction of the Finance department. They are valuable but are not adequate by themselves. The approach should always be conducted

collaboratively**.** Manual assessments include interviewing staff, performing **security** vulnerability scans, reviewing application and operating system access controls, and analyzing physical access to the systems.

A **Security Audit** is an extensive and formal overview of an organization's security systems and processes. The audit is an all-encompassing, in-depth, review of not only physical attributes, such as networks, firewalls, hardware, among others; but other areas including policy and standard operating procedures.

The term Security Assessment is generally referring to a Vulnerability Assessment which scans an organization's infrastructure and identifies vulnerabilities, such as faulty firewall, lack of system updates, malware, among others. With the assessment results, the technician can recommend steps to remedy the problems within the system.

Keep in mind, a Vulnerability Assessment is only a part of a **Security Audit**. Assessments can be performed individually, but they only cover one specific area. However, a **Security Audit** looks at all aspects of an organization's security rather than just scanning the systems currently in place.

A **Security Audit** consists of:

- Looking for holes in policy
- Physical Assessment (hardware, etc.)
- Access Control Assessment
- Vulnerability Assessment
- Design Controls/Processes
- Review of Standard Operating Procedures and Policies
- Review of Backup Disaster Recovery/Disaster Recovery Plan
    - This includes a Risk Assessment
- Configure Management
- Compliance Audit
    - HIPPA
    - 201 CMR 17
    - PCI DSS

A **Security Audit** consists of both a technical and conceptual overview of an organization's security systems and practices. A Vulnerability Assessment solely scans the organization's infrastructure and identifies flaws within the system.

Compliance is a critical component of any security program. The concept is that we must obtain evidence of **compliance** with implied policies, standards, laws, regulations, and other factors as well. Compliance is enforced by audits, which should be conducted internally and externally as well.

Every system, device, application, employee, and supplier can introduce cyber risk into a business's system. **Cyber Security Risk Assessment** of your organization's information assets should be protected and then the risk assessment investigates, identifies and analyzes the vulnerabilities existing within and around them.

Assessments deliver actionable recommendations to improve security, using industry best practices & the best technology available. A **threat assessment** is part of the overall **risk assessmen**t process; that is becoming more of a focus on security teams, who are prioritizing vulnerability remediation that is influenced by threats.

The core areas of a **risk assessment** are:

- Scope of Risk
- Data Collection
- Analysis of Policies and Procedures
- Threat Analysis
- Vulnerability Analysis
- Correlation and assessment of Risk Acceptability

They are utilized to help secure information on a company's infrastructure, so you must first understand how the network is configured, how it's used, and what is required to achieve security success. After establishing these items, it is important that the **risk assessment** be a collaborative process, without the involvement of various organizational levels, that the assessment can lead to a costly and ineffective security measure. Therefore, it is imperative that C-level leadership, the IT department, and the organization's security staff, need to be the ones that conjointly run a network **security assessment** together to gather:

- A deep dive review of devices configurations, software configurations and specific recommendations.
- Top-down analysis of Internet connectivity of DMZ and corporate to network devices, internal routing, and access controls.
- Analysis of servers, desktops, services, and applications.
- Vulnerability scanners, internal and external scanning appliances, may be used to identify vulnerabilities and misconfigurations.
- Intrusion Detection System appliances are used to monitor traffic and identify potential active threats and policy violations.

The outcome or objective of a **threat assessment** is to provide recommendations that maximize the protection of confidentiality, integrity, and availability, while still providing functionality and usability. To best determine answers to these questions a company or organization can perform a **threat** and **risk assessment**.

Determine Data Assets to be Protected

- Identify information assets within the primary types of information the organization handles
- Locate information assets based on where they reside within the organization
- Classify information assets in clear categories, such as public or regulated information

Determine Current Risk Levels

- Identify threats, vulnerabilities and describe risks
- Identify existing controls and determine likelihood of occurrence
- Determine severity of impact and assign risk level

Define Acceptable Risk and Recommend Safeguards

- Identify controls and recommended safeguards to reduce the risk presented by each threat/vulnerability pair
- Determine the residual risk level once the recommended safeguard is implemented
- Examine the likelihood of occurrence of the threat exploiting the vulnerability and the impact severity factors in categories of Confidentiality, Integrity, and Availability

Vulnerability analysis, also known as **vulnerability assessment**, is a process that defines, identifies, and classifies the security holes, vulnerabilities, in a computer, network, or any communications infrastructure. In addition, vulnerability analysis can reveal the effectiveness of proposed controls and evaluate their actual effectiveness after they are put into use. Technical, automated, scanning, is one piece of the puzzle, that gives a snapshot in time. It will not find all vulnerabilities, and may not detect input validation problems like SQL injections. One thing it does asses, is the system life cycle, development, and purchasing processes, as well as assess vulnerabilities in other processes, people, and physical sites.

Business Impact Analysis helps to align business continuity and IT disaster recovery plans to the value of the business processes being protected by identifying and evaluating the potential effects on financial, life/safety, regulatory, legal/contractual, reputation and so forth, of natural and man-made events on business operations. **Business Impact Analysis** also addresses IT complexity by supporting IT services, applications, data and underlying infrastructure classification. It reveals the bottom line if a vulnerability has been exploited.

A cybersecurity **risk assessment** is necessary to identify the gaps in organization's critical risk areas and to determine actions to close those gaps. It will also ensure that

time and money are invested in the right areas, so resources do not go to waste. **Risk assessments** combine Threat, Vulnerability, and Impact assessments, that need to be repeated to keep a system fully secure.

Insurance is designed to mitigate losses from a variety of incidents, including data breaches, business interruption, and network damage. A robust insurance market could help reduce the number of successful cyber-attacks by firstly promoting the adoption of preventative measures in return for more coverage. Second, it encourages the implementation of best practices by imposing premiums on the insured if the level of self-protection isn't sufficient. Many companies bypass policies, because of the perceived high cost of those policies, confusion about what insurance covers, and uncertainty that their organizations will suffer a cyber-attack. **Insurance** is usually appropriate for rare, high-impact events.

*** Our innovative solution to prevent users from being affected**

One of the biggest "gaps" that exist is that users often just do not care because they do not consider malware to be a real threat. An interesting way to show employees of a company just how easy it is to infect them is to get the IT department involved as white hat hackers. Businesses often provide company emails for their employees. An IT department could craft their own harmless "malware" and send them out to these employee emails. The email would include an attachment that looks somewhat familiar to and related to their work. The malware would not cause actual harm, but it would identify the employee that opened an attachment they should not have. Alternatively, the email can have a link to a website which could also identify which employee clicked on the link. This memorable approach of educating end users on the dangers of malware will show and involve the employees, allow them to learn from their mistakes, and show them what to avoid in the future.

Malware Conclusion

Many infections are contracted and spread by visiting gaming sites, porn sites, using pirated software (warez), cracking tools, hacking tools and keygens where visitors may encounter drive-by downloads through exploitation of a web browser or an operating system vulnerability. Security researchers looking at World of Warcraft and other online games and have found vulnerabilities that exploit the system using online bots and rootkit-like techniques to evade detection to collect gamer's authentication information, so they can steal their accounts.

There is no end to the channels through which malware can attack your computer, and once inside your system, these spread automatically and disrupts internet traffic as well. Some malware even gives access to your computer. Malware like Trojan horses do not replicate themselves, but they can damage a system badly and these generally come in the form of screensavers or free games. Fortunately, there are ways through which you

can protect your system from these malware attacks and you just need to be a little vigilant to avoid such attacks.

Resources

http://www.peachpit.com/articles/article.aspx?p=1960827&seqNum=5
http://combofix.org/how-malware-attacks-and-spreads-in-your-computer.php
http://www.sans.edu/research/security-laboratory/article/security-controls
http://www.lockheedmartin.com/us/what-we-do/information-technology/cybersecurity/tradecraft/cyber-kill-chain.html
http://www.DarkReading.com
http://www.csoonline.com/article/3004856/data-protection/the-dark-side-of-layered-security.html#tk.rss_all
http://www.ilpi.com/msds/ref/administrativecontrols.html
https://www.sans.edu/cyber-research/security-laboratory/article/security-controls
https://www.tracesecurity.com/services/it-security-audit
https://www.techopedia.com/definition/10236/information-security-audit
http://www.bureauveritas.com/home/about-us/our-business/cps/our-services/csr-services/security-audit
http://www.cutimes.com/2017/02/17/cybersecurity-compliance-more-important-than-ever
https://blog.volkovlaw.com/2016/01/cyber-security-compliance-role-cco/
https://www.sans.org/reading-room/whitepapers/auditing/overview-threat-risk-assessment-76
http://ww2.cfo.com/cyber-security-technology/2015/05/threat-assessment/
http://cdn2.hubspot.net/hubfs/1554068/Threat_Assessment.pdf?t=1476508559978
https://www.zuritechnologies.com/fortinet-cyber-threat-assessment/
https://www.secureworks.com/blog/vulnerability-assessments-versus-penetration-tests
http://www.continuitycentral.com/index.php/news/business-continuity-news/2422-using-business-impact-analysis-to-address-network-security-risks
https://www.kroll.com/en-us/what-we-do/cyber-security/prepare-and-prevent/cyber-risk-assessments
https://www.cio.com/article/2376802/security0/5-things-you-need-to-know-about-cybersecurity-insurance.html
http://www.datacenterjournal.com/ten-things-need-know-cybersecurity-insurance/
NIST IR 7298 Revision 2, Glossary of Key Information Security Terms
NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations

Preventative	Detective	Corrective	Compensatory
Security Awareness Training	System Monitoring	OS Upgrade	Backup Generator
Firewall	IDS	Backup Data Restoral	Hot Site
Anti-virus	Anti-Virus	Anti-Virus	Server Isolation
Security Guard	Motion Detector	Vulnerability Mitigation	
IPS	IPS		