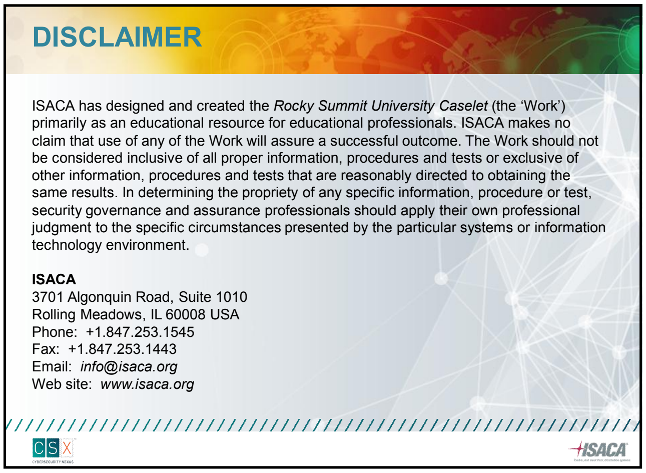
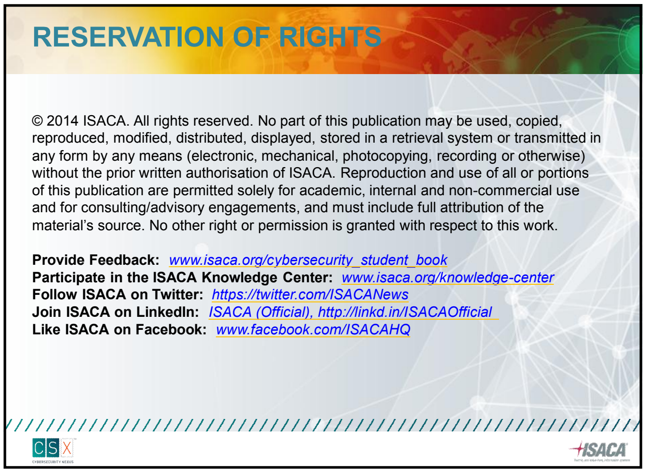
ROCKY SUMMIT UNIVERSITY: CYBERSECURITY THREAT, ATTACK AND DEFENSE MODELING CASELET



DISCLAIMER

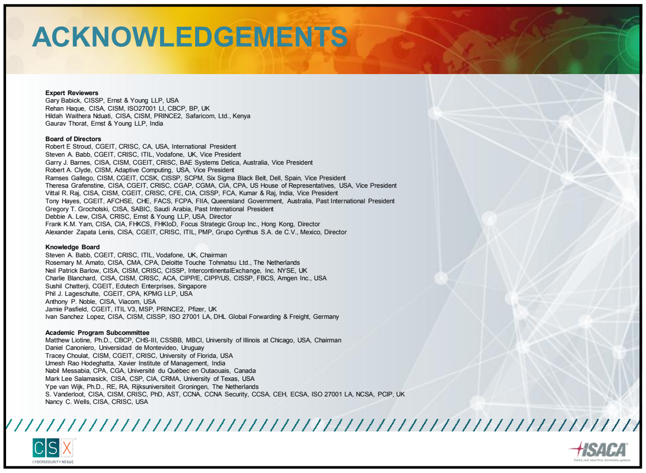
ISACA has designed and created the *Rocky Summit University Caselet* (the 'Work') primarily as an educational resource for educational professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, security governance and assurance professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: *info@isaca.org*
Web site: *www.isaca.org*



RESERVATION OF RIGHTS

Provide Feedback: *www.isaca.org/cybersecurity_student_book*
Participate in the ISACA Knowledge Center: *www.isaca.org/knowledge-center*
Follow ISACA on Twitter: *https://twitter.com/ISACANews*
Join ISACA on LinkedIn: *ISACA (Official), http://linkd.in/ISACAOfficial*
Like ISACA on Facebook: *www.facebook.com/ISACAHQ*



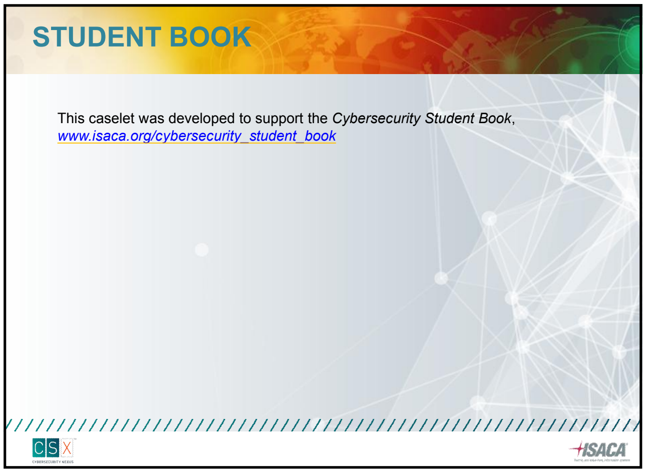
ACKNOWLEDGEMENTS

Expert Reviewers
Gary Babick, CISSP, Ernst & Young LLP, USA
Rehan Haque, CISA, CISM, ISO27001 LI, CBCP, BP, UK
Hildah Waithera Nduati, CISA, CISM, PRINCE2, Safaricom, Ltd., Kenya
Gaurav Thorat, Ernst & Young LLP, India

Board of Directors
Robert E Stroud, CGEIT, CRISC, CA, USA, International President
Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, UK, Vice President
Garry J. Barnes, CISA, CISM, CGEIT, CRISC, BAE Systems Detica, Australia, Vice President
Robert A. Clyde, CISM, Adaptive Computing, USA, Vice President
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, Six Sigma Black Belt, Dell, Spain, Vice President
Theresa Grafenstine, CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA, US House of Representatives, USA, Vice President
Vittal R. Raj, CISA, CISM, CGEIT, CRISC, CFE, CIA, CISSP, FCA, Kumar & Raj, India, Vice President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Past International President
Gregory T. Grocholski, CISA, SABIC, Saudi Arabia, Past International President
Debbie A. Lew, CISA, CRISC, Ernst & Young LLP, USA, Director
Frank K.M. Yam, CISA, CIA, FHKCS, FHKIoD, Focus Strategic Group Inc., Hong Kong, Director
Alexander Zapata Lenis, CISA, CGEIT, CRISC, ITIL, PMP, Grupo Cynthus S.A. de C.V., Mexico, Director

Knowledge Board
Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, UK, Chairman
Rosemary M. Amato, CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd., The Netherlands
Neil Patrick Barlow, CISA, CISM, CRISC, CISSP, IntercontinentalExchange, Inc. NYSE, UK
Charlie Blanchard, CISA, CISM, CRISC, ACA, CIPP/E, CIPP/US, CISSP, FBCS, Amgen Inc., USA
Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore
Phil J. Lageschulte, CGEIT, CPA, KPMG LLP, USA
Anthony P. Noble, CISA, Viacom, USA
Jamie Pasfield, CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, UK
Ivan Sanchez Lopez, CISA, CISM, CISSP, ISO 27001 LA, DHL Global Forwarding & Freight, Germany

Academic Program Subcommittee
Matthew Liotine, Ph.D., CBCP, CHS-III, CSSBB, MBCI, University of Illinois at Chicago, USA, Chairman
Daniel Canoniero, Universidad de Montevideo, Uruguay
Tracey Choulat, CISM, CGEIT, CRISC, University of Florida, USA
Umesh Rao Hodeghatta, Xavier Institute of Management, India
Nabil Messabia, CPA, CGA, Université du Québec en Outaouais, Canada
Mark Lee Salamasick, CISA, CSP, CIA, CRMA, University of Texas, USA
Ype van Wijk, Ph.D., RE, RA, Rijksuniversiteit Groningen, The Netherlands
S. Vanderloot, CISA, CISM, CRISC, PhD, AST, CCNA, CCNA Security, CCSA, CEH, ECSA, ISO 27001 LA, NCSA, PCIP, UK
Nancy C. Wells, CISA, CRISC, USA

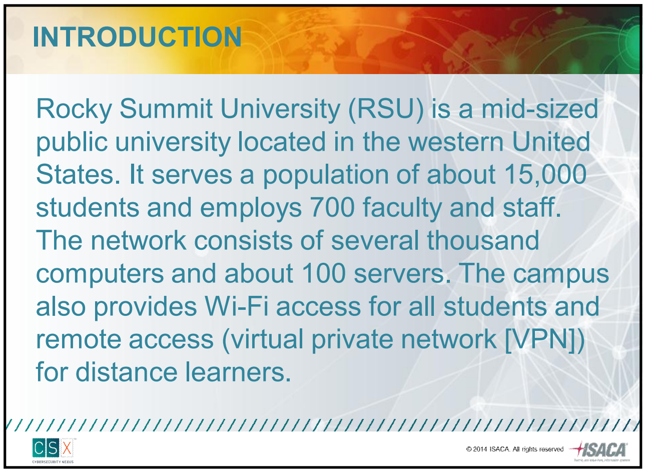


STUDENT BOOK

This caselet was developed to support the *Cybersecurity Student Book*, *www.isaca.org/cybersecurity_student_book*

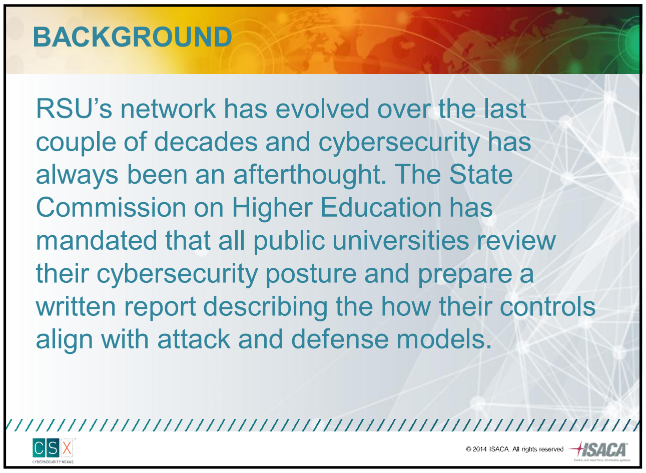
AGENDA

- Company Profile – Rocky Summit University
- Background Information
- Your Role
- Tasks
- Notes
- Glossary



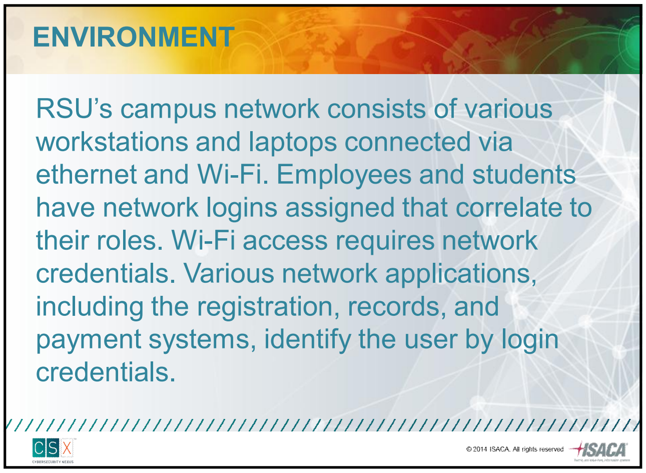
INTRODUCTION

Rocky Summit University (RSU) is a mid-sized public university located in the western United States. It serves a population of about 15,000 students and employs 700 faculty and staff. The network consists of several thousand computers and about 100 servers. The campus also provides Wi-Fi access for all students and remote access (virtual private network [VPN]) for distance learners.



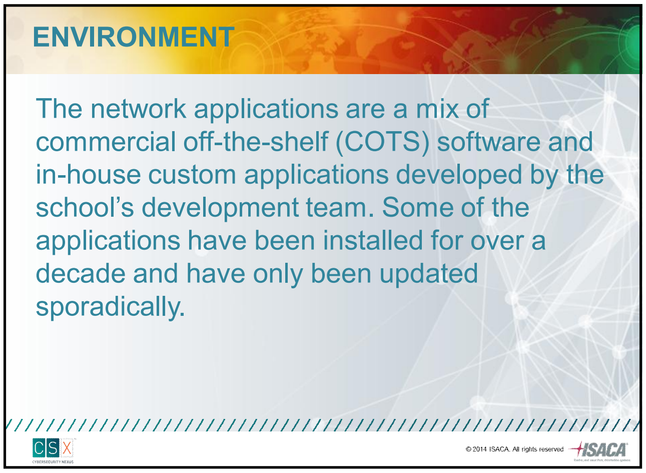
BACKGROUND

RSU's network has evolved over the last couple of decades and cybersecurity has always been an afterthought. The State Commission on Higher Education has mandated that all public universities review their cybersecurity posture and prepare a written report describing the how their controls align with attack and defense models.



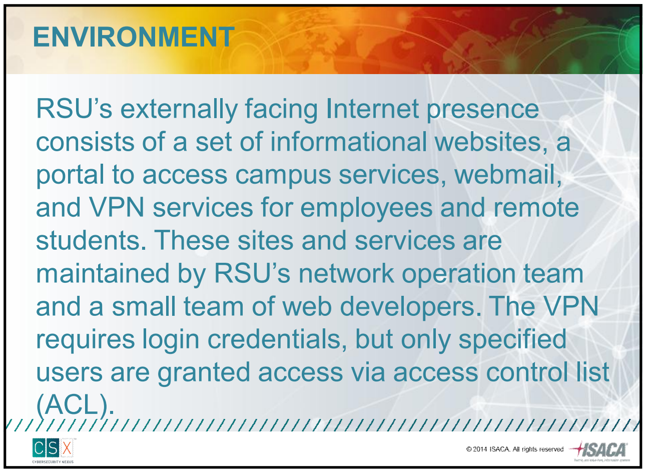
ENVIRONMENT

RSU's campus network consists of various workstations and laptops connected via ethernet and Wi-Fi. Employees and students have network logins assigned that correlate to their roles. Wi-Fi access requires network credentials. Various network applications, including the registration, records, and payment systems, identify the user by login credentials.



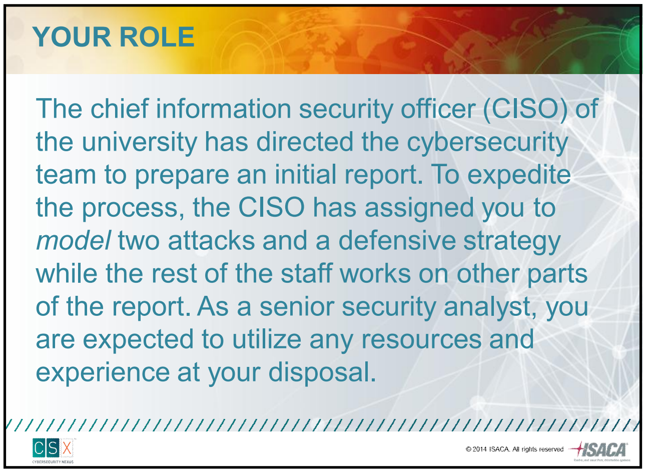
ENVIRONMENT

The network applications are a mix of commercial off-the-shelf (COTS) software and in-house custom applications developed by the school's development team. Some of the applications have been installed for over a decade and have only been updated sporadically.



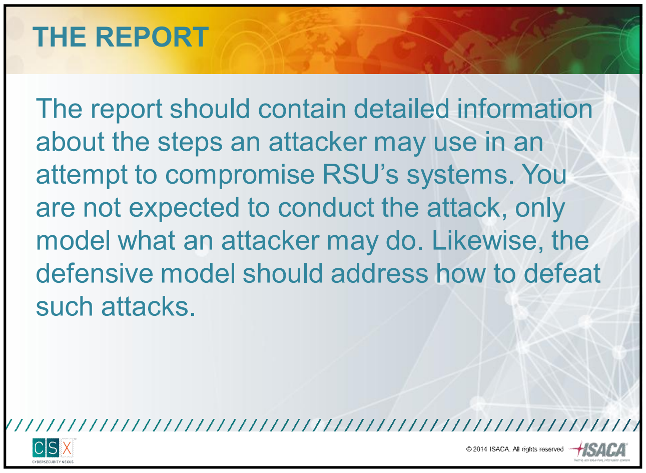
ENVIRONMENT

RSU's externally facing Internet presence consists of a set of informational websites, a portal to access campus services, webmail, and VPN services for employees and remote students. These sites and services are maintained by RSU's network operation team and a small team of web developers. The VPN requires login credentials, but only specified users are granted access via access control list (ACL).



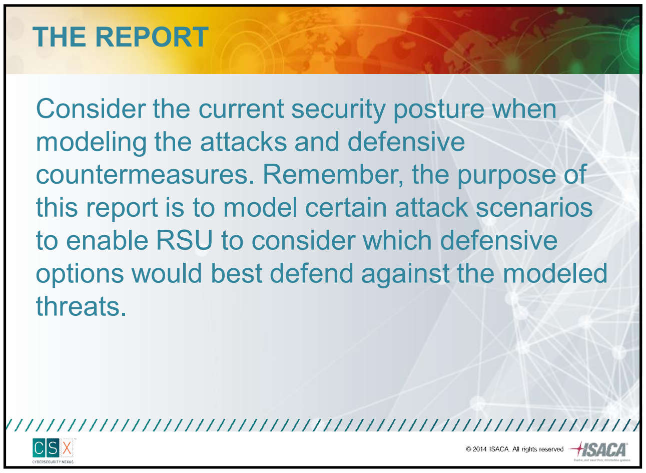
YOUR ROLE

The chief information security officer (CISO) of the university has directed the cybersecurity team to prepare an initial report. To expedite the process, the CISO has assigned you to *model* two attacks and a defensive strategy while the rest of the staff works on other parts of the report. As a senior security analyst, you are expected to utilize any resources and experience at your disposal.



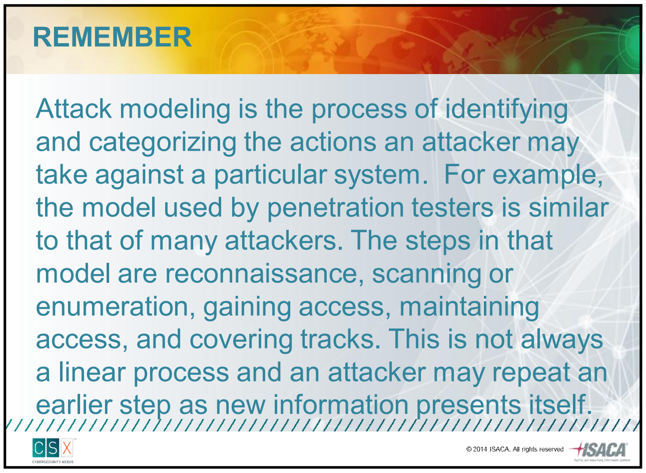
THE REPORT

The report should contain detailed information about the steps an attacker may use in an attempt to compromise RSU's systems. You are not expected to conduct the attack, only model what an attacker may do. Likewise, the defensive model should address how to defeat such attacks.



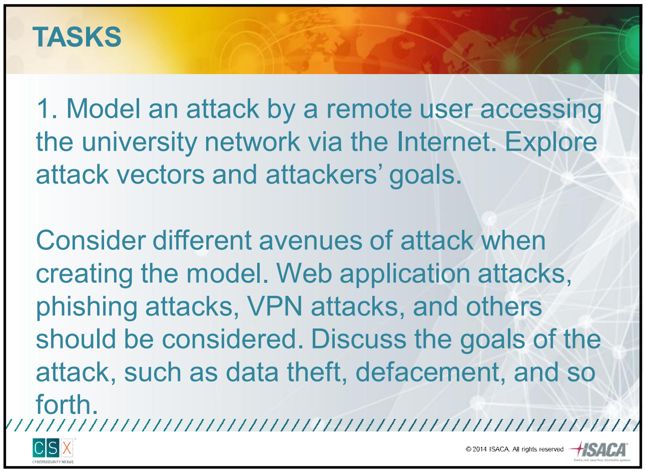
THE REPORT

Consider the current security posture when modeling the attacks and defensive countermeasures. Remember, the purpose of this report is to model certain attack scenarios to enable RSU to consider which defensive options would best defend against the modeled threats.



REMEMBER

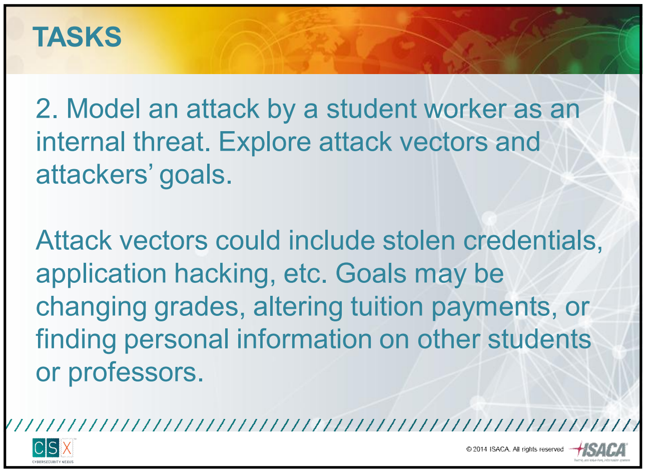
Attack modeling is the process of identifying and categorizing the actions an attacker may take against a particular system. For example, the model used by penetration testers is similar to that of many attackers. The steps in that model are reconnaissance, scanning or enumeration, gaining access, maintaining access, and covering tracks. This is not always a linear process and an attacker may repeat an earlier step as new information presents itself.



TASKS

1. Model an attack by a remote user accessing the university network via the Internet. Explore attack vectors and attackers' goals.

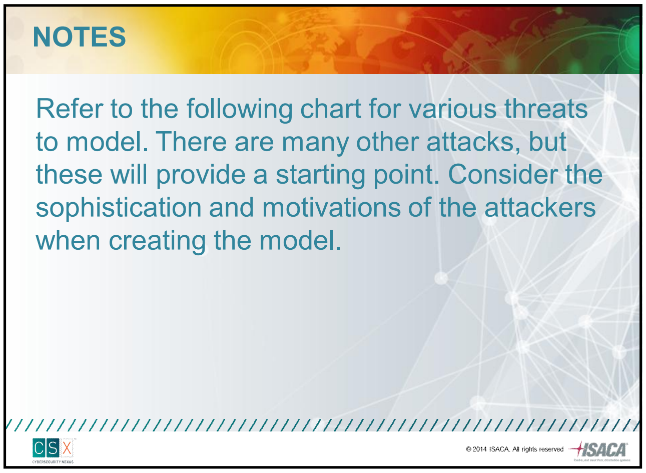
Consider different avenues of attack when creating the model. Web application attacks, phishing attacks, VPN attacks, and others should be considered. Discuss the goals of the attack, such as data theft, defacement, and so forth.



TASKS

2. Model an attack by a student worker as an internal threat. Explore attack vectors and attackers' goals.

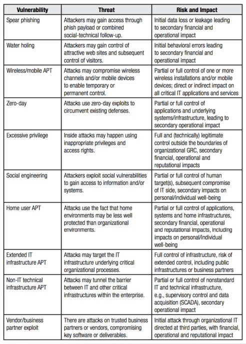
Attack vectors could include stolen credentials, application hacking, etc. Goals may be changing grades, altering tuition payments, or finding personal information on other students or professors.



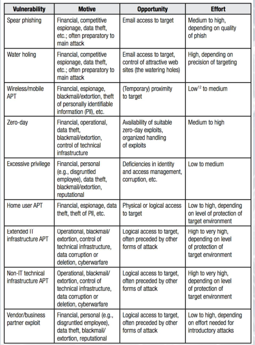
NOTES

Refer to the following chart for various threats to model. There are many other attacks, but these will provide a starting point. Consider the sophistication and motivations of the attackers when creating the model.

THREAT EXAMPLES



Vulnerability	Threat	Risk and Impact
Spear phishing	Attackers may gain access through phish payload or combined social-technical follow-up.	Initial data loss or leakage leading to secondary financial and operational impact
Water holing	Attackers may gain control of attractive web sites and subsequent control of visitors.	Initial behavioral errors leading to secondary financial and operational impact
Wireless/mobile APT	Attacks may compromise wireless channels and/or mobile devices to enable temporary or permanent control.	Partial or full control of one or more wireless installations and/or mobile devices; direct or indirect impact on all critical IT applications and services
Zero-day	Attacks use zero-day exploits to circumvent existing defenses.	Partial or full control of applications and underlying systems/infrastructure, leading to secondary operational impact
Excessive privilege	Inside attacks may happen using inappropriate privileges and access rights.	Full and (technically) legitimate control outside the boundaries of organizational GRC, secondary financial, operational and reputational impacts
Social engineering	Attackers exploit social vulnerabilities to gain access to information and/or systems.	Partial or full control of human target(s), subsequent compromise of IT side, secondary impacts on personal/individual well-being
Home user APT	Attacks use the fact that home environments may be less well protected than organizational environments.	Partial or full control of applications, systems and home infrastructures, secondary financial, operational and reputational impacts, including impacts on personal/individual well-being
Extended IT infrastructure APT	Attacks may target the IT infrastructure underlying critical organizational processes.	Full control of infrastructure, risk of extended control, including public infrastructures or business partners
Non-IT technical infrastructure APT	Attacks may tunnel the barrier between IT and other critical infrastructures within the enterprise.	Partial or full control of nonstandard IT and technical infrastructure, e.g., supervisory control and data acquisition (SCADA), secondary operational impact
Vendor/business partner exploit	There are attacks on trusted business partners or vendors, compromising key software or deliverables.	Initial attack through organizational IT directed at third parties, with financial, operational and reputational impact



Vulnerability	Motive	Opportunity	Effort
Spear phishing	Financial, competitive espionage, data theft, etc.; often preparatory to main attack	Email access to target	Medium to high, depending on quality of phish
Water holing	Financial, competitive espionage, data theft, etc.; often preparatory to main attack	Email access to target, control of attractive web sites (the watering holes)	High, depending on precision of targeting
Wireless/mobile APT	Financial, espionage, blackmail/extortion, theft of personally identifiable information (PII), etc.	(Temporary) proximity to target	Low[12] to medium
Zero-day	Financial, operational, data theft, blackmail/extortion, control of technical infrastructure	Availability of suitable zero-day exploits, organized handling of exploits	Medium to high
Excessive privilege	Financial, personal (e.g., disgruntled employee), data theft, blackmail/extortion, reputational	Deficiencies in identity and access management, corruption, etc.	Low to medium
Home user APT	Financial, espionage, data theft, theft of PII, etc.	Physical or logical access to target	Low to high, depending on level of protection of target environment
Extended IT infrastructure APT	Operational, blackmail/ extortion, control of technical infrastructure, data corruption or deletion, cyberwarfare	Logical access to target, often preceded by other forms of attack	High to very high, depending on level of protection of target environment
Non-IT technical infrastructure APT	Operational, blackmail/ extortion, control of technical infrastructure, data corruption or deletion, cyberwarfare	Logical access to target, often preceded by other forms of attack	High to very high, depending on level of protection of target environment
Vendor/business partner exploit	Financial, personal (e.g., disgruntled employee), data theft, blackmail/ extortion, reputational	Logical access to target, often preceded by other forms of attack	Low to high, depending on effort needed for introductory attacks

CSX CYBERSECURITY NEXUS

ISACA

REMEMBER

Defense modeling is often described as providing “defense-in-depth.” The concept of defense-in-depth is that the organization has several layers of defense that must be defeated for the attacker to be successful. For example, an organization can have a perimeter firewall, an intrusion detection system (IDS), a host-based firewall, and a patched operating system with unneeded services turned off.

CSX CYBERSECURITY NEXUS

ISACA

TASKS

Create a defensive model to address both threats, including details of the countermeasures and how they stop each step of the attack model.

(Hint: Internet searches may be useful in determining countermeasures for the modeled attacks.)

CSX CYBERSECURITY NEXUS

ISACA

NOTES

When modeling defense, consider each the steps of the attack and a control that can stop that step.

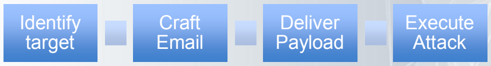
Layering these controls is key to defense-in-depth. If one of the steps in the attack fails, the attacker must find a new avenue for attack.

CSX CYBERSECURITY NEXUS

ISACA

EXAMPLE

An example spear phishing attack:

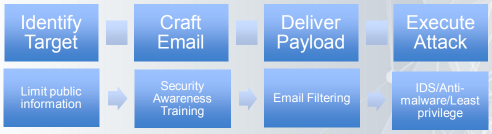


CSX CYBERSECURITY NEXUS

ISACA

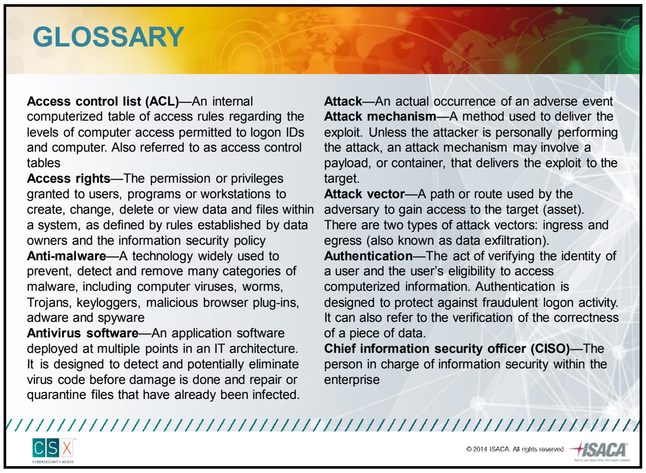
EXAMPLE

Defenses against example spear phishing attack:



CSX CYBERSECURITY NEXUS

ISACA



GLOSSARY

Access control list (ACL)—An internal computerized table of access rules regarding the levels of computer access permitted to logon IDs and computer. Also referred to as access control tables

Access rights—The permission or privileges granted to users, programs or workstations to create, change, delete or view data and files within a system, as defined by rules established by data owners and the information security policy

Anti-malware—A technology widely used to prevent, detect and remove many categories of malware, including computer viruses, worms, Trojans, keyloggers, malicious browser plug-ins, adware and spyware

Antivirus software—An application software deployed at multiple points in an IT architecture. It is designed to detect and potentially eliminate virus code before damage is done and repair or quarantine files that have already been infected.

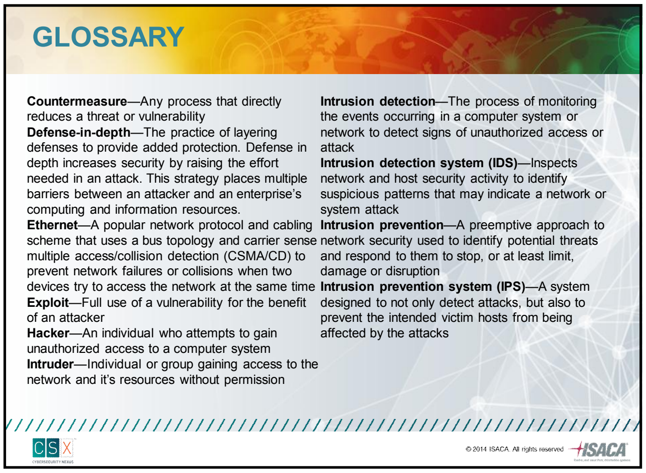
Attack—An actual occurrence of an adverse event

Attack mechanism—A method used to deliver the exploit. Unless the attacker is personally performing the attack, an attack mechanism may involve a payload, or container, that delivers the exploit to the target.

Attack vector—A path or route used by the adversary to gain access to the target (asset). There are two types of attack vectors: ingress and egress (also known as data exfiltration).

Authentication—The act of verifying the identity of a user and the user's eligibility to access computerized information. Authentication is designed to protect against fraudulent logon activity. It can also refer to the verification of the correctness of a piece of data.

Chief information security officer (CISO)—The person in charge of information security within the enterprise



GLOSSARY

Countermeasure—Any process that directly reduces a threat or vulnerability

Defense-in-depth—The practice of layering defenses to provide added protection. Defense in depth increases security by raising the effort needed in an attack. This strategy places multiple barriers between an attacker and an enterprise's computing and information resources.

Ethernet—A popular network protocol and cabling scheme that uses a bus topology and carrier sense multiple access/collision detection (CSMA/CD) to prevent network failures or collisions when two devices try to access the network at the same time

Exploit—Full use of a vulnerability for the benefit of an attacker

Hacker—An individual who attempts to gain unauthorized access to a computer system

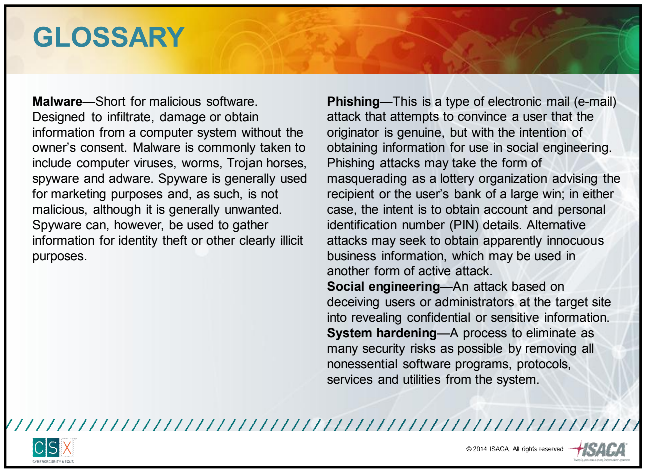
Intruder—Individual or group gaining access to the network and it's resources without permission

Intrusion detection—The process of monitoring the events occurring in a computer system or network to detect signs of unauthorized access or attack

Intrusion detection system (IDS)—Inspects network and host security activity to identify suspicious patterns that may indicate a network or system attack

Intrusion prevention—A preemptive approach to network security used to identify potential threats and respond to them to stop, or at least limit, damage or disruption

Intrusion prevention system (IPS)—A system designed to not only detect attacks, but also to prevent the intended victim hosts from being affected by the attacks



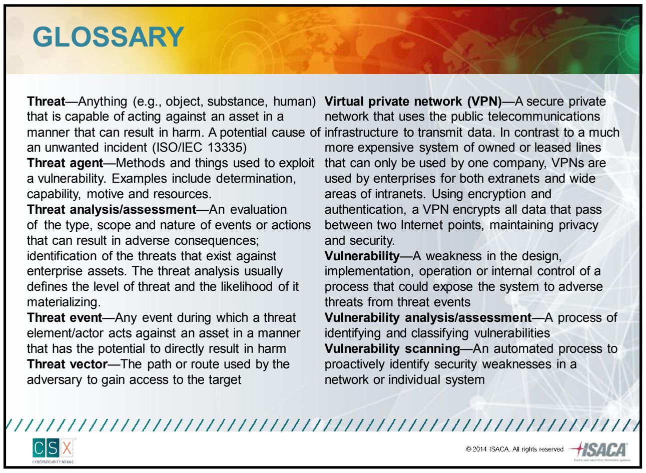
GLOSSARY

Malware—Short for malicious software. Designed to infiltrate, damage or obtain information from a computer system without the owner's consent. Malware is commonly taken to include computer viruses, worms, Trojan horses, spyware and adware. Spyware is generally used for marketing purposes and, as such, is not malicious, although it is generally unwanted. Spyware can, however, be used to gather information for identity theft or other clearly illicit purposes.

Phishing—This is a type of electronic mail (e-mail) attack that attempts to convince a user that the originator is genuine, but with the intention of obtaining information for use in social engineering. Phishing attacks may take the form of masquerading as a lottery organization advising the recipient or the user's bank of a large win; in either case, the intent is to obtain account and personal identification number (PIN) details. Alternative attacks may seek to obtain apparently innocuous business information, which may be used in another form of active attack.

Social engineering—An attack based on deceiving users or administrators at the target site into revealing confidential or sensitive information.

System hardening—A process to eliminate as many security risks as possible by removing all nonessential software programs, protocols, services and utilities from the system.



GLOSSARY

Threat—Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm. A potential cause of an unwanted incident (ISO/IEC 13335)

Threat agent—Methods and things used to exploit a vulnerability. Examples include determination, capability, motive and resources.

Threat analysis/assessment—An evaluation of the type, scope and nature of events or actions that can result in adverse consequences; identification of the threats that exist against enterprise assets. The threat analysis usually defines the level of threat and the likelihood of it materializing.

Threat event—Any event during which a threat element/actor acts against an asset in a manner that has the potential to directly result in harm

Threat vector—The path or route used by the adversary to gain access to the target

Virtual private network (VPN)—A secure private network that uses the public telecommunications infrastructure to transmit data. In contrast to a much more expensive system of owned or leased lines that can only be used by one company, VPNs are used by enterprises for both extranets and wide areas of intranets. Using encryption and authentication, a VPN encrypts all data that pass between two Internet points, maintaining privacy and security.

Vulnerability—A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events

Vulnerability analysis/assessment—A process of identifying and classifying vulnerabilities

Vulnerability scanning—An automated process to proactively identify security weaknesses in a network or individual system