RESILIA^{TM} – Certification Courses

Documents & Links

V1.01

Introduction & Use

This document is provided by your training provider as supplemental material to your Resilia certification course of study.

While not part of the course, its intent is to provide those new to the principles, concepts and practice of cybersecurity with a broad view of the current state-of-the-art.

The articles in this document will change as the practice of cybersecurity matures in its approach to cybersecurity threat at all levels.

Course Related Links

Blooms' Level Taxonomy

Bloom's Taxonomy provides an important framework for teachers to use to focus on higher order thinking. By providing a hierarchy of levels, this taxonomy can assist teachers in designing performance tasks, crafting questions for conferring with students, and providing feedback on student work This resource is divided into different levels each with Keywords that exemplify the level and questions that focus on that same critical thinking level. Questions for Critical Thinking can be used in the classroom to develop all levels of thinking within the cognitive domain. The results will be improved attention to detail, increased comprehension and expanded problem solving skills. Use the keywords as guides to structuring questions and tasks. Finish the Questions with content appropriate to the learner. Assessment can be used to help guide culminating projects. The six levels are: [Read more]

ITIL®

ITIL, formerly known as the **Information Technology Infrastructure Library**, is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business. In its current form (known as ITIL 2011 edition), ITIL is published as a series of five core volumes, each of which covers a different ITSM lifecycle stage.

ITIL describes processes, procedures, tasks, and checklists which are not organization-specific, but can be applied by an organization for establishing integration with the organization's strategy, delivering value, and maintaining a minimum level of competency. It allows the organization to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance and to measure improvement. {Read more]

ISO/IEC27001

ISO/IEC 27001:2005, part of the growing ISO/IEC 27000 family of standards, was an information security management system (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

ISO/IEC 27001 formally specifies a management system that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. Organizations that claim to have adopted ISO/IEC 27001 can therefore be formally audited and certified compliant with the standard. [Read more]

NIST – Framework for Cybersecurity Website

Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure, the President issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity, in February 2013. It directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure. [Read more]

NIST – Framework for Cybersecurity Document [PDF]

The Framework is a living document and will continue to be updated and improved as industry provides feedback on implementation. As the Framework is put into practice, lessons learned will be integrated into future versions. This will ensure it is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions. [Read more]

James Burke

James Burke (born 22 December 1936) is a British broadcaster, science historian, author, and television producer, who is known, among other things, for his documentary television series *Connections* (1978), and for its more philosophically oriented companion series, *The Day the Universe Changed* (1985), which is about the history of science and technology. *The Washington Post* called him "one of the most intriguing minds in the Western world." [Read more]

Geoffrey Moore

Geoffrey Moore (born 1946) is an American organizational theorist, management consultant and author, known for his work *Crossing the Chasm marketing and selling disruptive products to mainstream customers*. [Read more]

Agile

Most agile development methods break the tasks into small increments with minimal planning and do not directly involve long-term planning. Iterations are short time frames (timeboxes) that typically last from one to four weeks. Each iteration involves a cross-functional team working in all functions: planning, requirements analysis, design, coding, unit testing, and acceptance testing. At the end of the iteration a working product is demonstrated to stakeholders. This minimizes overall risk and allows the project to adapt to changes quickly. A single iteration might not add enough functionality to warrant a market release, but the goal is to have an available release (with minimal bugs) at the end of each iteration. Multiple iterations might be required to release a product or new features. [Read more]

The Deming Cycle

The PDSA Cycle is a systematic series of steps for gaining valuable learning and knowledge for the continual improvement of a product or process. Also known as the Deming Wheel, or Deming Cycle, the concept and application was first introduced to Dr. Deming by his mentor, Walter Shewhart of the famous Bell Laboratories in New York [Read more]

Deming; the man

He was an eminent scholar and teacher in American academia for more than half a century. He published hundreds of original papers, articles and books covering a wide range of interrelated subjects—from statistical variance, to systems and systems thinking, to human psychology. He was a trusted consultant to influential business leaders, powerful corporations and governments around the world. This includes inspiring and guiding the spectacular rise of Japanese industry after World War II, and the resurgence of the American automobile industry in the late 1980s. [Read more]

ADKAR Change Management Methodology

The ADKAR model is a results-oriented change management tool that is simple and easy to understand, yet very effective for managers and change management teams. We receive more calls for information about this model than any other. It is used as a resistance management tool, an assessment device and to help change management teams organize their work. [Read more}

Systems Thinking

Systems thinking is the process of understanding how those things which may be regarded as systems influence one another within a complete entity, or larger system. In nature, systems thinking examples include ecosystems in which various elements such as air, water, movement, plants, and animals work together to survive or perish. In organizations, systems consist of people, structures, and processes that work together to make an organization "healthy" or "unhealthy". Systems thinking has roots in the General Systems Theory that was advanced by Ludwig von Bertalanffy in the 1940s and furthered by Ross Ashby in the 1950s. The field was further developed by Jay Forrester and members of the Society for Organizational Learning at MIT which culminated in the popular book The Fifth Discipline by Peter Senge which defined Systems thinking as the capstone for true organizational learning. [Read more]

Kotter's 8-Steps

Over decades, Dr. Kotter observed the behavior and results of hundreds of organizations and thousands of leaders at all levels when they were trying to transform or execute their strategies. He identified and extracted the success factors and combined them into a methodology, the 8-Step Process. He then founded a firm of experts, Kotter International, to implement the approach across a diverse range of organizations. [Read more]

Cybersecurity in the News

Where Are We Now? The NIST Cybersecurity Framework One Year Later

The massive data breach at the U.S. Office of Personnel Management reportedly wasn't discovered by U.S. government sleuths - or the Department of Homeland Security Einstein intrusion detection system - but rather during a product demo.

Specifically, an April sales demonstration by Virginia-based CyTech Services of its digital forensics platform called CyFIR, which it used to scan the OPM network, unearthed a malware infection, which investigators now believe is tied to a network intrusion that began at least a year ago, *The Wall Street Journal* reports. [Read more]

Where Are We Now? The NIST Cybersecurity Framework One Year Later

The National Institute of Standards and Technology (NIST) released its Cybersecurity Framework (Framework) almost 15 months ago and charged critical infrastructure companies within the United States to improve their cybersecurity posture. Without question, the Framework has sparked a national conversation about cybersecurity and the controls necessary to improve it. In the past year, we have seen U.S. federal agencies and departments—as well as state governments and associations—engage and embrace the Framework for the various industries that they regulate. We discuss a few examples below. [Read more]

infoRisk ® Today

infoRisk Today is a multi-media website published by Information Security Media Group, Corp. (ISMG), a company specializing in coverage of information security, risk management, privacy and fraud. Headquartered in Princeton, New Jersey, USA, ISMG provides news, opinions, education and other related content to assist senior executives and information security professionals as they navigate the increasingly challenging world of information security. [Read more]

IRS: 100,000 Taxpayer Accounts Breached

Using personal information gained from third-party sources to circumvent **authentication** protections, hackers breached more than 100,000 accounts of taxpayers who had used the Internal Revenue Service's "Get Transcript" application, which has been temporarily shuttered. [Read more]

Large-scale attack uses browsers to hijack routers

Cybercriminals have developed a Web-based attack tool to hijack routers on a large scale when users visit compromised websites or view malicious advertisements in their browsers. [Read more]

Cybersecurity Awareness

End Users Must Be Part of Cyber Security Solution

As the old InfoSec adage goes, “people are the weakest link in the cybersecurity chain.” Clearly, enterprise security professionals agree with this statement. In a recent ESG research survey, enterprise security professionals were asked to identify the factors most responsible for successful malware attacks. It turns out that 58% point to “a lack of user knowledge about cybersecurity risks” – the most popular answer by far *(note: I am an employee of ESG)*. [Read more]

Awareness is Key

As pressure from regulatory compliance increases the modern chief information security officer (CISO) must take an increasingly holistic and integrated approach to information risk management. By implementing strong information security measures, the CISO is more likely to stay ahead of regulatory mandates. [Read more]

Gartner Article on IT Spending ...especially for security

On Monday during the Gartner Symposium/ITxpo in Orlando, Peter Sondergaard, senior vice president at Gartner and global head of research, told an audience of more than 8,000 CIOs and IT leaders that worldwide IT spending is expected to reach $3.8 trillion in 2014, up 3.6 percent from 2013. However what’s getting IT leaders excited is the opportunities that await in the new, emerging era of the Digital Industrial Economy. [Read more]

The Cost of Cyber Breaches

Hackers have made the Internet a scary place to do business, as recent headlines attest. Big companies have been hacked. Small companies have been hacked. As the Pew Research Internet Project reported earlier this week, cyberattacks are likely to get worse.

How much should a small business spend to protect against cyber villains? I asked Eric Montague, president of Executech, an IT firm in South Jordan, Utah, for an estimate. While the answer will vary, depending on the type of business—not to mention the relative optimism of its owner—Montague’s response offers a useful baseline: Some $57,600 a year for a 50-employee company. [Read more]

Government research reveals true cost of cyber crime

A survey conducted on behalf of Get Safe Online (a jointly funded initiative between several government departments and private security businesses) to coincide with Get Safe Online Week has found that 51% of those surveyed experienced online crime, of whom only 32% reported the crime. 47% of victims did not even know who to report an online crime to. [Read more.]

Utility meters at risk of cyber attack

A utility company based in Spain is now looking to improve its smart meters after security researchers found flaws in the devices. This story highlights the growing issue surrounding the security of the 'Internet of Things' [Read more]

Cyber security – 7 facts your board needs to be aware of

With data breaches hitting the news headlines almost on a daily basis, it is shocking that global security budgets fell 4% in 2014 compared with the year before, according to a new PwC survey of almost 10,000 executives. The report reveals that the number of reported security incidents increased by 48%, to 42.8 million, the equivalent to 120,000 attacks a day. Meanwhile, the average cost of managing and mitigating data breaches rose to $2.7m per incident, over a third more than in 2013.

With these controversial figures in mind, the need to change the board's view on cyber security is urgent. Here are seven facts your board needs to be aware of: [Read more]

Lessons Learned

Cyber security – Lessons from Target's Data Breach Tumble

As the risk of data breaches are on the rise exponentially, so are the number of attacks and financial impact on American businesses. My intuition and experience in the field just make me wonder, how big it is and plan strategic is going on and what the end purpose is just probably unknown for now, but one thing is sure, it is not just for the Money, but a bigger impact such as an economic impact in a County, in a region or even globally. [Read more]

The 15 Worst Data Security Breaches of the 21st Century

Data security breaches happen daily in too many places at once to keep count. But what constitutes a huge breach versus a small one? For some perspective, we take a look at 15 of the biggest incidents in recent memory. Helping us out are security practitioners from a variety of industries, including more than a dozen members of LinkedIn's Information Security Community, who provided nominations for the list. [Read more]

56% of cyber criminals cited Christmas as the best time for corporate hacking

Hackers love the winter holidays. Obviously, they enjoy crisply crunching through silent snowdrifts and warming themselves in ancient inglenooks as they knock back mulled wine and roasted chestnuts while raucously singing carols – that goes without saying. But they also love the increased criminal opportunities the holidays bring.

The festive period is frequently cited by cyber criminals as the best time of the year to engage in corporate hacking. Indeed, a 2009 survey of anonymous Defcon attendees found that 56% of cyber criminals thought the winter holidays the optimal time to hack corporate computers. Why? [Read more]

Tyupkin ATM Malware; Banks Give Away Cash

Eastern European malware allows attacker to steal 40 bank notes of the highest value in the machine from any infected ATM.

Have you ever wanted to withdraw cash without the debit appearing on your account? How about investing in a key that will allow you to rob ATMs? [Read more]

The Insider Threat: Is It Avoidable?

News has emerged in the last couple of days about two cases of data breaches caused by insiders. The two incidents make for an interesting comparison.

In one of these cases an innocent employee of JP Morgan Chase was the victim of a social engineering attack and having a weak password. While this wasn't a malicious act, the mistake led to the theft of 76 million customers' data. [Read more]

JPMORGAN ATTACK:
Developer's password gave alleged Russian hackers broad access to data

As the New York Times reported, "Until just a few weeks ago, executives at JPMorgan said they believed that only one million accounts were affected, according to several people with knowledge of the attacks." The problem then seemed to be relatively contained — if you regard one million records compromised as manageable in terms of a data breach in the modern age.76 million, of course, is one quarter of the population of the United States. [Read more]

Your medical record is worth more to hackers than your credit card

Security experts say cyber criminals are increasingly targeting the $3 trillion U.S. healthcare industry, which has many companies still reliant on aging computer systems that do not use the latest security features.

"As attackers discover new methods to make money, the healthcare industry is becoming a much riper target because of the ability to sell large batches of personal data for profit," said Dave Kennedy, an expert on healthcare security and CEO of TrustedSEC LLC. "Hospitals have low security, so it's relatively easy for these hackers to get a large amount of personal data for medical fraud." [Read more]

Senators ask Apple, Home Depot for information on breaches

A recent data breach at retailer Home Depot and a leak of celebrity nude pictures from Apple's iCloud service raise questions about the companies' data security practices, two U.S. senators said Thursday. Two lawmakers ask the companies to explain the cause of recent data breaches. [Read more]