Cyber Security for the Project Manager: Am I at Risk? [1]

By John Cable, Director

Project Management Center for Excellence
A. James Clark School of Engineering
University of Maryland, USA

In our 2021 Virtual Project Management Symposium, Susan Parente, Engineer and Consultant, spoke on this topic during her presentation, titled "*Cyber Security for the Project Manager: Am I at Risk?*" And we would like to share this important knowledge with you.

Susan Parente has a wide area of expertise that includes project risk management and IT security, as well as 15 certifications (including 10 Agile certifications and 4 IT security/ risk certifications) for professional education and teaching purposes. She has more than 25 years of experience leading software and business development projects in the private and public sectors and has 2 decades of experience implementing IT projects for the DoD and other federal government agencies. Parente is a consultant, author, teacher, and speaker in the fields of Program and Project Management, Agile Project Management, and Risk Management (both Project Risk Management and IT Security). She is currently working on program management support for a cybersecurity effort, completing independent verification and validation testing of systems for FEMA.

Coming from the fields of Project Management and IT Security, Susan has found that people have a lack of knowledge when it comes to IT Security, and she strives to bridge that gap. Speaking on "Common Threats and Vulnerabilities", She defines some terms within the Cybersecurity world. *Phishing* is described as the fraudulent practice of sending email that is masked as coming from a viable source, with the goal of having individuals divulge personal information. These emails need to be looked at closely for any discrepancies or information that doesn't look quite right, such as the sender's email address. Parente notes that this tactic is very commonly used and unfortunately often works. *Social Engineering* is another deception by fraudulent parties to manipulate someone into sharing personal information or confidential information (sensitive data). With this there is a sense of urgency and threat of some negative outcome used to get people to provide personal information. Those who are not computer savvy, such as

[1] How to cite this article: Cable, J. (2021). Cyber Security for the Project Manager: Am I at Risk? Commentary, *PM World Journal*, Vol. XI, Issue II, February.

seniors, are often a target. Spyware and the Trojan Horse are malicious programs packaged in what appears to be legitimate software (including games or software marketed to be helpful to the user). These will run in the background and spy on your computer system or may even delete files.

Continuing with the shared terms on cybersecurity threats; *Viruses* are hidden in software, infecting one's computer and attempting to spread to all on your contact list. *Ransomware* is another type of malicious software which is used to hold your computer data ‘hostage’ until you provide a payment to release it and regain access to your computer. This is another great reason to back-up your data. A *Worm* is a virus which is a program that infects your computer and then works on its own and propagates, by sending itself to other computers. A *DoS*, or *Denial of Service*, *Attack* has the specific goal of hitting a particular website or server until the volume of hits takes the system down, thus denying service to others.

So, why is Cybersecurity so important? Susan Parente helps in answering this question for ourselves by providing a deeper look into this field and the threats within. She first notes that Cybersecurity, a.k.a Information Technology Security, is made up of the techniques that protect computers, networks, programs and data from unauthorized access or attacks on one’s computer or systems. A *Cyber Attack* is an attempt to cause damage or destruction to a computer system or network. Cyber-attacks can target an individual or an entire organization with the intent to disrupt, disable, destroy, or control a computer, its environment, or infrastructure, destroy the integrity of data, or steal information.

Susan moves on to discuss the threat of *Attacks and Breaches*. An Attack is the attempt to gain unauthorized access to information or services, or to harm IT systems. A *Breach* is an incident that ends in an *attack* as a result of bypassing the security structure of the system. Susan quotes an important datapoint from Verizon’s 2015 Data Breach Investigations Report that states, “90% of successful cyber-attacks succeed because of human error”. She then provides an example of these ‘human errors’ that she has personally encountered in her work. Parente explains that within organizations people have access to different systems of the organization and when they leave the company their account to these systems is sometimes not removed. This is a concern and a potential threat because an account that no one is using is “like a key to your house being left somewhere in your yard”. It only takes a smart enough person to look under the rock or planter to find the key. It is more obvious if someone has gotten into an account that is regularly used because someone can quickly identify that something is wrong.

Susan draws on voices across various fields in our modern-day society to emphasize the weight cybersecurity holds. First up is Professor Angela Sasse, professor of Human-Centered Technology at UCL and Director of the UK Research Institute in Science of Cyber Security (RISCS). Professor Sasse is quoted: “You need to really work with your people and embark on conversations with them about the threats that are out there. That’s what we want to change - we want people to talk about security, discuss the risks, but help each other out. The more people talk about security with each other, the better things will become.” Parente then quotes Warren Buffet: “It takes 20 years to build a reputation and 5 minutes to ruin it. If you think about that, you’ll do things differently.”

Susan directs an important question toward her audience, “What are we doing in our organizations to support our reputation that we have, to protect assets, and information?” Parente has done several training classes in New York City for an organization within the financial industry where she observed papers left out on desks and computers left logged in and walked away from. She reminds you to avoid these risky habits! Lastly, Tom Farely, President of the New York Stock Exchange, is quoted, “It is important companies remain vigilant, taking steps to proactively and intelligently address cybersecurity risks beyond the technological solutions, we can accomplish even more through better training, awareness and insight on human behavior. Confidence, after all, is not a measure of technological systems, but of the people entrusted to manage them.” Susan urges that we can no longer claim to not have to worry about IT security just because “there’s a department for that”. It is our job to take precautions because the data is in front of us at our desks and on our computer screens.

Again, “Why is Cyber Security so important?” Susan has no intent to scare you, but to increase awareness and keep IT Security in mind. She urges that you know IT security requirements at the beginning of projects, during software development, *before* getting into production. Susan elaborates on what we can do now. To prevent attacks there need to be risk assessments that looks at vulnerabilities of systems, planning for what can be done should an attack occur, and a promotion of awareness, so people can act proactively. Responding to attacks relies on recognizing an attack and detection of intrusions or malware. General prevention includes IT Security Guidelines and Standards that should be developed and implemented to prevent and manage IT security for the organization. Password Safety should be established and entail guidance in the creation and management of high-strength passwords to help stop attackers from gaining unauthorized access to the organization’s network. Lastly, Remote and Mobile Working require the safe use of office devices outside of the organizational environment.

The prevention of attacks demands Risk Identification. The identification, of these Cyber Security risks, relies on Operations Cyber Security Risks (as per SEI). This includes the actions of people, including unintentional, intentional, and lack of action; Systems and Technology Failures, including hardware, software, and systems; Failed Internal Processes, including design of processes, execution of processes, controls for processes, and supporting processes; and External Events, including hazards, legal, business, and dependencies of services. Alongside Risk Identification is Risk Awareness. This entails both Enterprise Security Risk Assessment, to include an assessment of both probability and impact to evaluate the risk exposure; and Risk Response Planning, for those vulnerabilities which are above the organizational or project risk tolerance. Where are the risks coming from? Both intentional (hackers, criminals, terrorists, etc.) and unintentional (human error by employees or contractors) sources. The overall process is to identify, assess, plan response, execute, and repeat - which applies to both Project Risk Management and IT Security Risk Management.

Susan Parente concluded with a few clear messages. She stakes her claim that employees are your most effective defense and stresses the importance of Security Awareness Training at the recommended 1-2 times per year to avoid unintentional human error. Parente highlights that Cybersecurity is very necessary - and the threat is very real - but risks can be greatly reduced through security awareness. She notes on her experience with the UMD Project Management Symposium sessions that she “loves the mixture of educational and professional information” and encourages you to attend!

The next University of Maryland *VIRTUAL* Project Management Symposium will be May 5-6, 2022. The event will feature 4 keynote speakers and 55 individual sessions in 5 concurrent tracks. Event information will be available September 1, 2021. If you want access to all 57 of the session recordings from the 2021 event at very low cost, visit the 2021 Project Management Symposium website to register.

About the Author

John Cable

Director, Project Management Center for Excellence
University of Maryland, College Park, MD, USA

John Cable is Director of the Project Management Center for Excellence in the A.James Clark School of Engineering at the University of Maryland, where he has been a professor and teacher of several graduate courses in project management. His program at the University of Maryland offers masters and PhD level programs focused on project management. With more than 1,300 seats filled annually with students from many countries, including more than 40 PhD students, the program is the largest graduate program in project management at a major university in the United States.

John Cable served in the newly formed U.S. Department of Energy in 1980, where he was involved with developing energy standards for buildings, methods for measuring energy consumption, and managing primary research in energy conservation. As an architect and builder, Mr. Cable founded and led John Cable Associates in 1984, a design build firm. In 1999 he was recruited by the University of Maryland's Department of Civil & Environmental Engineering to create and manage a graduate program in project management. In his role as founder and director of the Project Management Center for Excellence at Maryland, the program has grown to offer two undergraduate minors, 3 master's degrees, and a doctoral program. Information about the Project Management Center for Project Management at the University of Maryland can be found at www.pm.umd.edu.

In 2002, PMI formed the Global Accreditation Center for Project Management Educational Programs (GAC). Mr. Cable was appointed to that inaugural board where he served as vice chair. In 2006, he was elected as chairman, a role he held through 2012. As Chair of the PMI GAC, John led the accreditation of 86 project management educational programs at 40 institutions in 15 countries in North America, Europe, the Middle East, Latin America and the Asia Pacific Region. John was awarded PMI's 2012 Distinguished Contribution Award for his leadership at the GAC. He can be contacted at jcable@umd.edu.

To view other works by John Cable, visit his author showcase in the PM World Library at https://pmworldlibrary.net/authors/john-cable/