Security for the 21st Century and Beyond: A Call To Action [1]

By Eddie R. Williams

Contributing Author: Marc Gravez

As organizations and companies address security (which includes cyber security) during and beyond the 21st century, this article is a call to action for the Project Management Institute (PMI), other project and program management organizations, and companies in various industries.

This call to action, if implemented, would result in all appropriate projects and programs having a security plan.

Keep H. O. P. E. Alive: High Octane (Performing) Program/Project Execution

Gartner continues to emphasize the importance of security and risks: https://www.gartner.com/smarterwithgartner/gartner-top-7-security-and-risk-trends-for-2019/

Commentary

This is an opportunity to ensure security is addressed/covered for projects and programs and in an organization/company. However, be aware this is also an opportunity for hackers and those with malicious intent to disrupt business, political activities (such as elections) and to increase cyber security attacks/activity. Hackers and those with malicious intent could have a field day if we do not address security and change our cultures to ensure security is a way of life in the operation/conduct of any business, onsite or remotely.

Many businesses understand the seriousness of planning and implementing strong security to counter threats, but some may not have met the challenges for the 21st century and beyond.

Note: I have worked for companies in several industries. Each organization addressed security differently, which is understandable because their needs/requirements vary. One item missing from every project/program was a security plan (document). To some degree,

[1] How to cite this article: Williams, E. and Gravez, M. (2020). Security for the 21st Century and Beyond: A Call To Action; Commentary, *PM World Journal*, Vol. X, Issue I, January.

all were addressing security but the planning phase for IT or business transformation projects/programs had no plan dedicated to security.

PMI calls out several plans/documents in the PMBOK such as

- Stakeholder Plan
- Risk (and Issue) Plan
- Communication Plan
- Change Management Plan
- Other plans

My career started in an environment where lives, safety and security were priorities. For several projects and programs that I successfully managed through close out, the following additional plans were created:

- RACI/RASCI (important for responsibility/accountability)
- Security Plan (allows a project/program to address security at the organization, application/system, infrastructure/network level or all levels)

Security concerns exist because we know it is about securing data/information.

Security is a business and technical concern. It affects not only the technology but impacts business operations. The more computer systems and technology changes through upgrades and innovations the more risks/issues and problems can affect business operations and the bottom line.

Are you security ready? Companies in all industries must be "security ready" now and for the near future and beyond. There must be policies, plans and procedures that address and implement security in companies and industries.

Have you performed assessments through TOPP (Technology, the Organization, People (knowledge base and skills), and Processes (business processes) to identify the risks associated with security being implemented in a company and for a project and program? If not to some degree, do it/or perform assessments and evaluation leading to execution/implementation of a security program.

Are you educating and training your organization? You must begin to consider not only project and program changes but also organizational, enterprise-wide security training. Change management must lead this effort.

Conduct and perform testing and piloting that are planned (in an Agile, Waterfall or hybrid manner). Adequate testing and qualifying activities must be implemented before you put products and systems into production.
Many project and program managers understand why security requires coverage. In some industries, it is emphasized with guidance from subject and security matter experts. We all need to realize that introducing more technology increases the importance and urgency of security. We must create a culture of security, with an attitude by employees,

consultants, managers and others through education, training and coaching, etc. that creates the appropriate behavior.

Quality, whether top-down or bottom-up, begins with an individual.

How can we support security, privacy and confidentially, integrity, and availability of data/information? We know how important this is for healthcare systems, defense systems, communications systems, gaming, etc. It is also about developing and producing systems that are reliable.

Project and program management – Security planning and analysis must be performed and a plan created to ensure security is addressed and implemented whether for on premise or the cloud, along with strong access and authentication and authorization implementations.

The following are what is being addressed or what is required at a minimum (the experts in/outside of your organizations know/or should know what is required).

Organization

a. Ensure security is part of strategic planning
b. Establish/create policies and have them immediately implemented
c. Establish a data/information security governance entity
b. Ensure that security is established enterprise/company-wide
c. Where applicable/appropriate, institute “passwordless” technology
c. Train/educate on a continuous basis
d. We know that there is no 100% guarantee of security but a company can be diligent about its implementation with some of the activities below and keys areas identified in many companies/articles we can be on top of things for the 21st century and beyond.

1. Prevention
2. Detection
3. Disaster Recovery and Testing and Business Continuity
4. Incident Reporting
5. High Level Encryption
6. Biometric Access
7. Stronger Hardware and Software Based Authentication
8. Physical Security
9. …

Applications and System Software

All applications and system software must be secure

a. All developed applications and systems and products must be developed and produced with security built in
b. Application integration systems must be validated

c. This security is implemented with other communications/social media applications/systems such as Facebook, Google, Twitter, Zoom, WebEx, Skype, etc.
d. Remote communication must be verified and validated for security purposes
e. All systems must be verified and validated before use with thorough QA/testing.

Infrastructure/Networks and Communications Systems

All infrastructure hardware and software must be secure

a. All infrastructure hardware (servers, communication equipment and systems must be installed and verified and validation before production use)
b. All telecommunications systems must be validated for Local and Wide Area Networks security and communications
c. Remote systems must be verified and validated for security purposes with thorough QA/Testing

Culture of Security

a. Create a security conscious culture through continuous education, training and improvement activities

Quality and security is an attitude, a state of mind!

CALL TO ACTION

PMI (And Other Project and Program Management Organizations)

1. PMI, and other project and program management organizations, must address and add a Security Plan as one of the required plans (e.g., stakeholders, risk/issues, communication, change, etc. (and now a security plan)) identified as a project/program deliverable. During my career, I have added security planning to ensure that security was addressed and documented. I have been a certified PMI PMP for over 15 years (and still active) without a break in certification. This recommendation comes from my experience and background.
2. A security plan that considers the above areas (under Security Concerns…), and when not applicable can be identified as not applicable.
3. The information can also be created as a checklist.
4. Do not just emphasize education and training but also suggest that they are conducted on a periodic or some required basis.
5. …

Companies

1. What companies must do is create, or continue to create, a security policy considering at a minimum the above areas.

2. Although security must be addressed for all projects and programs, the content document would apply where appropriate (e.g., organization, application/system software, infrastructure/network) and where not applicable indicate.
3. A security plan, an accepted or approved document, which may be affected by security policy changes and changes in an organization and technical risks.
4. Expect and require that a security plan be a result of security planning and assessment/evaluation.
5. Create templates as required.
6. Continue, as many companies are, to have education and training on security, like HIPAA. Ensure it is mandatory for home system users also because you know how we tend to say too many meetings, etc. to attend. Give the employees, consultants, and managers an opportunity to receive training (as some companies have done) with consequences if they are not responsible/accountable.
7. Now we have to address security for other mobile devices such as phones, tablets, watches, etc.
8. Implement a total quality management system (does not have to be a TQM). It was a system like TQM at a company I worked for in the beginning of my career that provided me the opportunity to suggest/recommend that a RACI/RASCI and Security Plan be created for projects that required security to be addressed/implemented.
9. …

Note Only:

Home/remote system users – Companies are having employees, consultants and managers work from home now because of Covid-19.

Many home computer/system users must address security. They are also using cell phones, tablets, and watches for communication.

1. Household systems must be secured, and internet connections verified and validated
a. Secure internet connections
b. Update systems as required
c. Use and update virus applications (latest versions and its security)
d. Scan frequently
e. …

Note: I upgraded my home system/network environment for example, within my budget. You can only do what your budget allows. I ensured that my cable company had the necessary speed and bandwidth I required and I upgraded my Ethernet cables. Since I did not want to use the modem-router of the cabling company, I bought and set up a new & upgraded router (my firewall) with high encryption. Since my wife was now working from home, purchased a new computer system (all-in-one desktop) for her to work from home and to remotely access her company computer/network through her client application. Now she can use her laptop more for her personal use and crafts.

I recommended that she create strong/stronger passwords. Her company now is planning to provide her and other employees with company systems to use from home. I assume there are individuals and many companies taking similar steps. Less or more depending on a budget and what the companies are doing/providing.

Conclusion

Security as we know it today will continue to be a critical concern. It must be built in, continuously improved, driven by policies, identified and documented in a plan for projects and programs. Now, surely being considered when implementing big data storage, the cloud and/or hybrid systems. …and covid-19 has affected all industries such as critical healthcare, pharmaceutical and financial services, etc. Who is not impacted?

Create a security conscious culture. There is no guarantee for 100% security, but implement secure business and technology environments. Where appropriate, create an enterprise policy. For any project or program, ensure that security planning takes place and a resulting plan is created based on the project/program requirements.

Any feedback or comments are encouraged. If I am off base or on the wrong track, please advise.

What I live by: My mother always said that you have not lived a full life unless you have reached out to help/assist someone/others. She said you cannot change the world but if you reach out to help/assist someone or others, maybe they will be inspired to help/assist someone or others.

Eddie R. Williams, PMP

About the Authors

Eddie R. Williams

New Jersey, USA

Eddie R. Williams, PMP has over 25 years of experience as a program and project manager for system/software engineering, Information Technology (IT) development and management in aerospace, DOD, commercial IT and other industries such as healthcare, pharmaceutical, insurance, and academia. He has been a Project Manager, Sr. PM, Program Manager, Sr. Program Manager, Integration Manager, and Sr. Program/Portfolio Manager for the creation, development and management of PMOs/EPMOs. He has managed successfully through close out projects and programs for business transformations and systems, applications (including web applications) and infrastructure/networks, communication systems implementations. Mr. Williams has been a certified Project Management Professional (PMP) through the Project Management Institute since 1999. Before becoming a certified project and program manager, he held positions such as Systems and Procedures Analyst (programming and creating system/software specifications), Configuration Management Specialist and Manager, Software Product/Quality Assurance Engineer and Manager, Division Administrator/Manager (development methodologies (Waterfall, Agile, hybrid, etc.), management and control).

He is also a coach/mentor and educator, and been a speaker at numerous conferences, and is the author of Software/Firmware Configuration Management (Within the System Development Process) and Management Control and Quality. In 2014, he provided program management content through the Program Management Academy: Content contribution to the 2014, Wiley publication, “Program Management for Improved Business Results" for University master’s degree programs. Eddie can be contacted at http://www.itprofessionalfacilitator.com.

Marc Gravez

Pennsylvania, USA

Marc Gravez is a customer-focused technical communication professional and technical writer. His passion is creating content that empowers people to learn faster,

remember more, and work better, bridging the gap between what users know and technologists think users know. Mr. Gravez has more than 20 years of industry experience, including healthcare IT, telecom, cable, networking, banking, and engineering. He is a Past President of the Society for Technical Communication (STC) Philadelphia Metro Chapter. He can be contacted at marcgravez@gmail.com.