Could Your Project be the Reason for a Data Breach?

Eben Berry
President and Founder of Cyber Inspectors™ LLC
eben.berry@cyberinspectors.com

Mr. Berry formed a new venture enabling companies to have greater preparedness in responding to growing concerns with cyber-attacks. As a former CISO, his twenty three years of experience across Military, Fortune 1000 and non-profit organizations centered on business, technology and information security. He received his MBA from Northeastern University.

Ehsan Sabaghian
VP of Business Development of Cyber Inspectors™ LLC
esabaghian@cyberinspectors.com

After receiving his 2nd master's degree in information technology management from Clark University, MA. Mr. Sabaghian joined Cyber Inspectors LLC. An information systems expert with extensive background in business management, he emerged as a strong change agent SME on many large IT projects.

Published in projecttimes.com – December 2011.

The Challenge and It's Scale

A Project Management Office (PMO) leader gets a call from her boss who just found out that a recent web portal service delivered by one of her project teams has been compromised by an ever growing population of cyber attackers. If this was your project, how would you respond to a call from your PMO leader? What due diligence can you reference showing that you incorporated essential security practices in protecting a strategic business revenue generating asset? In USA Today, a title in the Money section of August 12, 2011 reads, "8M Web Pages Hacked, Mined". If you think this could not happen to your projects, think again. Organizations and career professionals who manage and make decisions regarding existing and newly deployed strategic assets must take a different delivery approach to further minimize significant impacts that lead to lost revenue and front page news stories.

Project managers have been traditionally driven by on-time and on-budget performance metrics rather than also including security as a top priority metric for project management deliverables. This results in making an organization's strategic assets easy targets for cyber attackers. Out of all data breaches investigated in 2010 by Verizon Business, 96% were avoidable. (Source: 2011 Verizon Business Data Breach Investigations Report). Cyber-attacks are real and will continue to target organizations of all sizes, regardless of the industry. Organizations and project managers must take a different approach in delivering cyber safe assets to the Internet. New organizational performance metrics for cyber safety will become mandatory in determining overall project and corporate success. Competitive advantage, in the age of cyber threats, will determine success for organizations and career professionals who take a proactive approach to cyber security. "Under the evolving landscape, organizations require a new business approach in providing a greater level of trust, safety and security for their customers as they extend higher quality solutions to Internet-based services," says Eben Berry president and founder of Cyber Inspectors™ LLC.

Cyber Security's Emerging and Prevalent GAP

The expanding gap for organizations today starts with consumer driven markets and stakeholder pressure to offer differentiated services that grow the bottom and top lines of the business. In order to stay competitive, many new business and delivery models have leveraged the Internet, outsourcing, offshoring, cloud based services and mobility platforms that continue to outpace the reach of cyber security. A 2011 CIO cloud survey by CIO.com stated that 71% of enterprises had placed security among their top three concerns related to moving to the cloud. These strategic business decisions have created invisible windows that have opened gaps in making organizations easy targets for cyber attackers for the assets they deploy. The model has completely shifted to an open versus closed system, enabling an unprecedented level of access to sensitive information within companies and business partners today. Most organizations do not have the required visibility, knowledge, talent or capability to ensure cyber safe practices are incorporated throughout the planning, delivery and operating life cycles. Given the sophisticated techniques used by cyber attackers, organization and career growth will depend on how well companies and career professionals embrace their roles by enhancing their delivery competencies and skills. Organizations have become more data-dependent. It has been estimated that just over the last two years, the data footprint used by organizations across the globe has doubled (Berkeley School of

Info Management and Systems 2009). Although organizations and business leaders cannot disrupt services to customers, they can take the first step to make cyber security a strategic priority in the planning and delivery process. Acquiring new knowledge and having an informed mindset is the starting point in combating the new epidemic of cyber threats. Understand your current mindset by testing your knowledge today with the quick self-assessment below:

What Do the Numbers of Cyber Threats and Attacks Tell Us

Cyber threats and attacks are real and here to stay. The few statics we have shared below include just some highlights gleaned from thousands of breaches worldwide. Cyber Attackers may not always have a preference and consider no target too big or too small. These targets include projects, career professionals and organizations. One of the many statistics that directly applies to project delivery includes 6,253 new vulnerabilities discovered in 2010 (Published in Apr 2011, Symantec Internet Security Threat Report).

Many of these vulnerabilities go undetected during the project and software development lifecycle phases. Data theft reported last year due to these vulnerabilities being compromised has impacted on average 260,000 identities per breach. (ibid Apr 2011) Not only market pressure but rising legal precedence with new federal and state regulations has raised the stakes for all organizations and career professionals. The numbers over the past few years continue to show a rising trend of successful cyber-attacks with no end in sight. Organizations and career professionals can no longer afford being reactive and must take a proactive approach in delivering strategic assets cyber safe.

Test <u>Your</u> Cyber Security Knowledge; Answer Yes or No.

1. Do you know what you should track and trace throughout your project delivery regarding cyber security risks and threats?
2. Do you know the difference between cyber threats and attacks?
3. Do you know the techniques cyber attackers use to compromise organizations and assets delivered by projects?
4. As the project leader, can you determine with little effort what data and records may have been exposed by a cyber-attack based on the project data you included in your project delivery plan?
5. Do you know what your internal incident response team will ask of you?
6. Can you validate to external auditors and investigators that you took the appropriate due diligence in delivering a cyber safe project?
7. Do you conduct privileged penetration testing to determine if exploitable vulnerabilities may expose sensitive data used in your project solution to cyber threats?

Your response and understanding of these questions begins to illustrate the gaps you may have regarding the level of cyber safe practices in your project, business and career. If you answered "no" to one or more of these questions, you may have a project <u>already</u> at risk of being compromised by cyber attackers.

In the next section, we will review our approach to assist career professionals such as project managers on how to begin delivering better cyber safe solutions and the value it delivers to project quality. Organizations that embrace and apply this new approach will begin to reposition cyber security as a business advantage instead of being reactive to the market causing significant financial loss and consumer trust impacts.

The Solution and It's Value

Viewing Cyber Security as a Business Solution

The advancements in technology have both enabled organizational strategies but have come with a price to pay with the advancements of cyber threats. Hence, cyber security is a moving target with no final technological solution for it. Considering the rate of progress in new technologies and their social prevalence, the solution is now more dependent on people's mindset, their critical thinking abilities and requires greater individual responsibility. These facts lead us to believe that the most effective resistance against cyber threats must now be built on shifting an individual's mindset, adjusting human behavior and evolving legacy methodologies. Cyber security has elevated as a must have for businesses and career professionals. Therefore, cyber safe practices require a proactive approach in solving a new set of cyber breach business challenges associated with strategic asset delivery and survivability. The first important step project managers can take starts with making cyber security a priority and positioning cyber safe practices as part of the solution in the upfront initiation and planning processes. Project Managers and delivery team professionals such as business analysts should also incorporate cyber security safe practices into the remaining project phases ensuring traceability of established cyber security requirements.

Gartner research study conducted in 2010, reactive versus proactive investment in cyber security could have up to a 70 to 1 price tag. Many of the cyber security challenges that organizations face today have less to do with a technology problem and more to do with the human element and process approach as being the weak link. An older but still relevant report on the leading causes of data loss included 1 in 2 events had been caused by human error and 1 in 4 related to a policy violations (Source: IT Policy Compliance Group). This speaks directly to a need for greater awareness, education and a new business approach to delivery strategic assets cyber safe.

Protecting business assets that live in today's evolving dangers of the Internet and mobility infrastructure requires a unified approach across business, IT and security in maintaining business resistance to cyber threats and attacks. As an example to clarify, a window in your house that protects you from weather damage, heating and cooling costs, and unwanted intruders. This requires a set of combined controls involving human process and technologies. These controls include cyber security (i.e., requiring a particular lock be part of the design), IT controls (i.e., incorporating the lock into the window design), and the business controls (i.e., ensuring that a daily routine has been established to shut and lock the windows). Without the unified business approach and controls in place from all three areas, organizations can increase their risk of water damage, higher heating and cooling bills and enable intruders to have easy access.

- **A Mindset Shift, Behavior Modification and Methodology Change**

To truly change the advantage cyber attackers have today, managers and individuals require a shift in their mindset towards cyber safety. Although many see cyber security as a technological problem data breaches have shown society that this has become more of a human behavior problem. Many organizations continue to rely on their employees as their last line of defense but most non-technical roles in the organization do not have the required awareness and education that is required to fully minimize an organizations exposure to cyber threats and attacks.

This demands a new business awareness, delivery and operational approach to expand an organizations capabilities and competencies for both non-technical and technical career professionals such as project managers. A new set of data handling and safeguard skills for all employees' and third party vendors for handling sensitive data in cyber space has become a fundamental organizational requirement. Business units, business projects and entire organizations must improve preparation by investing in new cyber safe practices training, education and certification programs. This mindset shift, behavioral modification and methodology change should then be followed up with actionable techniques.

A New Market Business Delivery Assurance Model™; Designing your Projects and Solutions Cyber Safe

Businesses need to take a proactive approach to cyber security and develop a business delivery assurance model tailored to their industry and organization. This model places an emphasis on designing, building and Growing Secure Business™ rather than reacting to data breaches and exposures that your business could have avoided.

Innovating a New Delivery Assurance Model through Cyber Security

Cyber security must become part of every career professional's mindset in further shifting an organization to a security minded culture. In order to level the playing field and begin building resistance against cyber attacks, asset protection demands a multi-dimensional model that includes individuals, organizations and society. In order to gain significant advantage quickly, a new set of baseline standards must be created for organizations to better evaluate the technology vendor selection process to ensure a particular vendor's solution does not become the reason for a data breach. This becomes even more critical to organizations that have shifted or making the shift to mobility platforms to enable new business model innovations.
Hence, the birth of this new Business Delivery Assurance Model developed by Cyber Inspectors™ LLC that provides a holistic approach in blending cyber security essential safe practices with well tested business delivery models. Acquiring new knowledge of cyber security through education

and coaching has become essential in maintaining new skills and techniques for delivering cyber safe solutions. Establishing cyber safe planning and delivery performance metrics, empowering your project teams by making security a priority and incorporating cyber safe practices into your business process designs will result in putting your organization in a more defensible position. Once you begin acquiring the necessary knowledge in raising visibility of these elusive threats, organizations and career professionals will see how easy this can be to incorporate into the planning, delivery and operational process deliverables.

Cyber Security and Project Management: The Perfect Partnership

Assuming that three of the main project management functions are managing resources, managing project risk and managing project quality assurance, let's review potential business risk impacts of cyber threats and attacks created during the project delivery life cycle. (See Table 1.0: Cyber Security and Project Management)

Project Management Functions	Cyber Threat & Attack Impacts	Cyber Safe Practice Examples
Managing Resources	Data Loss Exposure Identities and Intellectual Property Stolen	Incorporate Essential Practices for Project Data Cyber Safe Data Assurance Management Plan
Managing Project Risk	Erosion of Customer Trust Brand Image Impacts Stakeholders' Dissatisfaction	Establish Cyber Security Priorities Establish Cyber Safe Performance Metrics
Managing Project Quality Assurance	Low Quality Projects: Open Windows Low Quality Deliverables: Easy Targets Inadequate testing of threats	Incorporate Scenario Based Threat Testing Develop Cyber Deliverables Checklist Develop Business Incident Response Plan

Table 1.0: PM Functions, Cyber Threat and Attack Impacts and Cyber Safe Practice Examples

Cyber Security and Project Management: A New Delivery Benchmark

The well-known Project Management triangle (Scope, Schedule and Cost) requires a new business protection benchmark that includes a cyber-security layer. This new project metric (See diagram 1.0) enables organizations, PMO's and delivery teams to position a higher level of business delivery assurance related to the quality of projects. This builds stakeholder and customer confidence that organizational assets have been delivered cyber safe. Current business performance metrics for PMOs and Project Leaders mainly measure success by on-time and on-budget. Given the significant financial impacts felt by organizations caused by cyber attacks, project leaders can begin making the difference by incorporating a new delivery benchmark for cyber safe practices. This will position project and career success by building a resistance to cyber attacks within the strategic assets deployed. Once you have put this new approach into action, project managers will begin to minimize putting their projects, organizations and vendor partners at risk of failure and exposure to cyber breaches.

Project Leaders can begin incorporating cyber safe delivery practices by including this new formula. (See diagram 1.0)

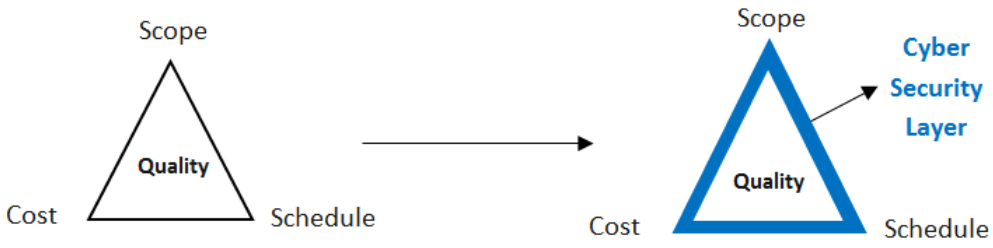


Diagram 1.0: Project Delivery Cyber Security Layer

Cyber Security Added Value for Project Managers

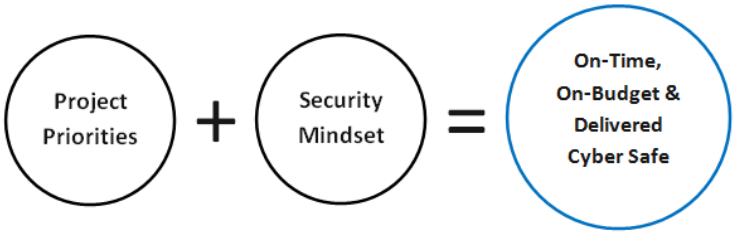
Cyber security is no longer a debated option, it is essential to operate and grow business in the digital age of cyber threats and attacks. Growing your business and workforce more securely creates economic value immediately related to cost avoidance and revenue driven by customer trust. Making cyber security a strategic priority enables new business expansion and builds your organizational bench strength to carry out strategic objectives required for sustainability against the evolving dangers of the digital cyber space. For PMO leaders and project managers this provides career advantages and positions new opportunities for organizations that have successfully made the shift.

How Cyber Security Adds Value for Projects		
Assets / Resources	**Not Cyber Safe**	**Cyber Safe**
Project Data	Significantly increases a project's risk in becoming a cyber threat	Establish cyber safe data life-cycle practices
Project Deliverables	Can increase exposure to cyber exposing access to an organizations crown jewels	Incorporate essential cyber security practices as part of the project and process deliverables
Project Technology Environments	Lack of production controls in development and testing environments creates an easy target for cyber attackers	Monitor use and minimize the use of live data across all non-production environments and validate that productions controls are in place and tested
Project Vendors	High potential of being the weak link and entry point for cyber attackers	Establish cyber security SLAs with penalties and incorporate essential practice language in agreements
Project Mobile Devices	Expands and exposes your vulnerabilities to an increased level of threats and attacks	Perform vendor due diligence and conduct threat based scenario testing of mobile solution based on business use cases
Project Members	Limited or lack of cyber security awareness, training and coaching can lead to a higher likelihood of cyber breaches	Conduct cyber safe practice orientations and invest in training on what project members must know regarding delivering cyber safe solutions
Your Project	**Project Failure and Data Exposure**	**On-Time, On-Budget & Cyber Safe Project Delivery**

[Table 1.0] Cyber Safe Added Value for Project Managers

Cyber Safe, a New Project Management Metric

Cyber security must be part of your solution going forward to remain competitive, to retain your constituent trust and attract the top talent required to compete in the Internet market. Do not wait until your project or organization's assets have been compromised by cyber attackers to begin making an essential business practice shift. Begin establishing and incorporating your delivery process with cyber safe essential practices today. Minimize your chances in being a target and establish cyber safe as a new benchmark for project management success. Organizations and career professionals, including executives, must make cyber security a priority by investing upfront in the strategic planning and delivery process to integrate cyber security as a competitive advantage in the products and services they offer. Project Managers who armed themselves with cyber security knowledge and techniques will begin to deliver higher quality projects, increase their marketability and help PMs in achieving greater career success.



(Diagram 2.0: Cyber Inspectors LLC Formula for Delivering Cyber Safe Solutions)

Disclaimer: *The information presented in this article is intended as general advice. Specific advice would require Cyber Inspectors LLC to become familiar with the facts of you or your organization's particular situation. Please do not attempt to apply the general advice presented to your situation until after you have consulted Cyber Inspectors or another qualified person and fully explained the important facts.*

About Cyber Inspectors™ LLC. Founded in 2011 and based in Burlington, MA, Cyber Inspectors is focused on cyber security and enabling companies to achieve greater organizational preparedness in responding to cyber threats and attacks. Cyber Inspectors has developed a new Business Delivery Assurance Model™ focused on cyber safe essential practices, response capabilities and strategic investment of security.

Visit Our Website: http://www.cyberinspectors.com/?page_id=18