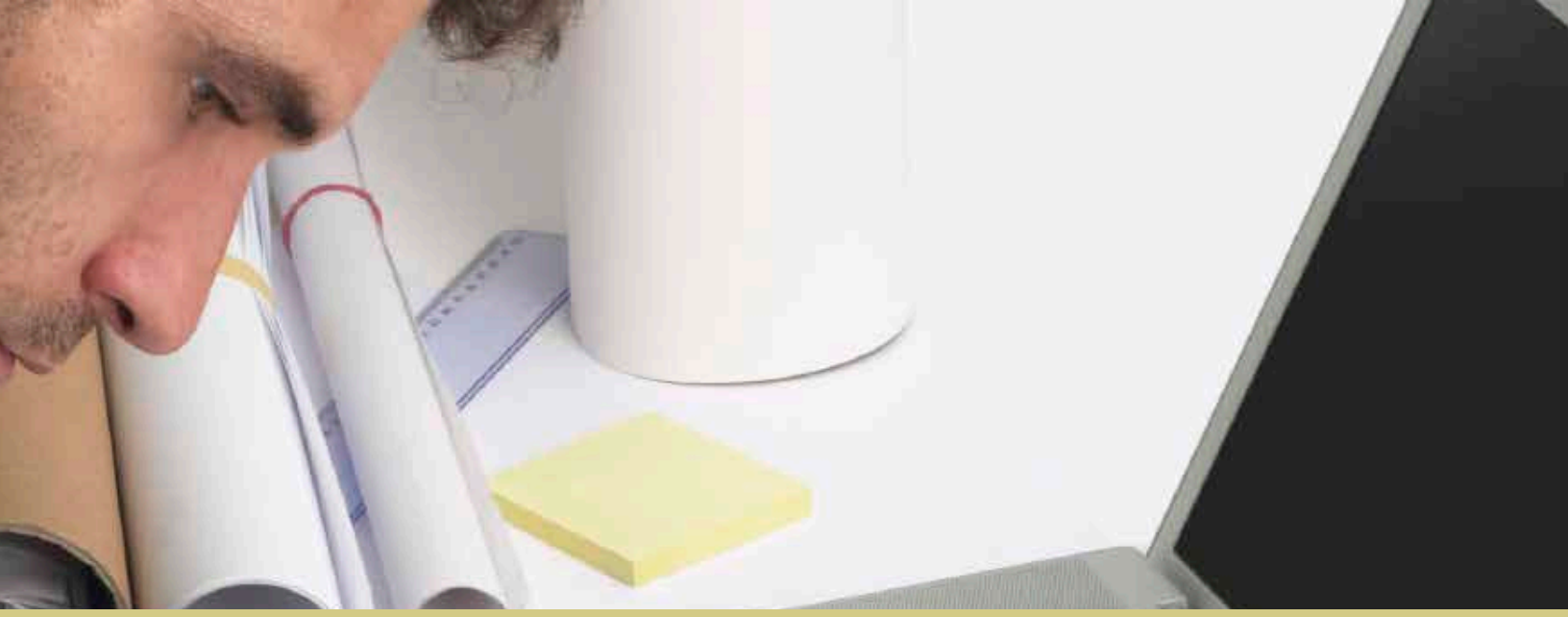

Cybersecurity on Your Project:
Why Not Follow National Security Strategy?

Prepared by:
Rick Erickson
Snell & Wilmer L.L.P.

LORMAN®

Published on www.lorman.com - December 2018

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 1300 available
- ☑ **Slide Decks -** More than 2300 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

Cybersecurity on Your Project:
Why Not Follow National Security Strategy?

*Written by **Rick Erickson** – 8/20/18*

In its recent *Cybersecurity Strategy*, the U.S. Department of Homeland Security (DHS) defined "cyberspace" as "the independent network of information technology infrastructure, including the Internet, telecommunications networks, computers, information and communications systems, and embedded processors and controllers." To DHS, protecting cyberspace includes threats against "federal and nonfederal information systems." In other words, both private and public interests are at risk. In his 2018 *National Defense Strategy*, U.S. Department of Defense Secretary, Jim Mattis, essentially concurred in declaring cyberspace a "warfighting domain" and promising to "invest in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations."

The construction industry is a key player in cybersecurity because contractors, designers and owners are responsible for building and delivering projects providing critical public services like national defense, health care, law enforcement, transportation, and utilities. Like any business reckoning with risks in cyberspace, moreover, everyone on a construction project has valuable data and confidentialities to protect. Cyber breaches on a project may also compromise electrical power, physical safety and, inevitably, a lot more than the critical path schedule and profit margins. Cybersecurity

insurance is not very affordable or comprehensive, either, and it usually excludes any property damage or bodily injury resulting from a cyber event.

A quick read of the *Baidu, Inc. v. Register.com, Inc*. case is enough to alert any company how a low-level employee's failure to follow simple cybersecurity protocols can compromise a company's entire network and trigger significant damages claims by third parties for the breach. It is also important to recognize that Target's 2013 data breach, which compromised millions of customers' credit information, was accomplished by stealing access information from an HVAC contractor working on Target projects. No doubt, the HVAC contractor was uninsured for any negligence in getting hacked and could hardly stand with Target to compensate millions of consumers for their losses.

When considering cybersecurity liabilities, therefore, it can't hurt to exemplify those who have the most to protect. Consider that our defense agencies, which have the highest calling of national security, may have a risk assessment and prevention model that transcends to the construction industry. For example, DHS's "five pillars" approach to achieving national cybersecurity goals can be analyzed and applied to cybersecurity risks in construction as follows:

1. **Risk Identification**

Everyone on a construction project has to know what the cybersecurity risks are before they can prevent them. At all levels of construction operations, the players also have to agree there is a risk worth preventing. Stolen bid information can destroy a contractor's competitive edge. A hacker's compromise of an electrical grid can

shut down the entire project indefinitely. Unrestricted use of personal electronic devices on a project can potentially expose an owner's company network to cyber breaches. Cyber criminals are endlessly trolling for windows of opportunity to exploit network gaps and hold a company up for ransom. In construction, therefore, the first step is to have frank discussions about the most obvious and most complex risks posed to your company's cyber welfare.

Along the same lines as DHS's guidance on risk identification, the discussion has to include how cyber threats have evolved in a way that can be crippling to the business and its reputation in the industry. Project owners will probably ask, while engaging in their due diligence, whether your cybersecurity measures and protocols are up to snuff. If your construction company devotes little to cybersecurity and has been subject to cyber events, it may cost you the project. Be ready to affirm that you have identified cyber risks to prevent them from impacting all involved.

2. **Vulnerability Reduction**

Unless you hire an expert with qualifications and experience in protecting public and private information systems, you will probably not reduce your company's cyber vulnerability. Investing in a Chief Information Officer (CIO) for the project may reduce your premiums for cybersecurity liability insurance and will help impress upon all players that you are less vulnerable to cyber breaches. Bring your CIO to planning meetings, and make it known that you are committed to reducing cyber vulnerabilities in specific ways.

Regular training and written policies are also a key to reducing vulnerability. In the same way training contributes to a viable safety

plan for the project, training in cybersecurity contributes to development of protocols designed to reduce cyber vulnerabilities. Good cybersecurity also depends on each individual recognizing their part in securing computers, devices and proprietary information from open viewing and access. The project's job trailers, offsite workspaces and meeting rooms need to be treated more like cybersecurity vaults than break rooms and general office space. This is one of many, tedious changes that must be made.

3. **Threat Reduction**

Leaders in the construction industry can deter cyber threats by combining forces. That is, a combined effort against hackers and other cyber criminals may force them to focus their efforts elsewhere—to more isolated, vulnerable and unsuspecting victims. Sharing information about cyber events, contingencies and solutions can only help to reduce the threat. In addition, a joint effort will assist law enforcement in identifying targets for prosecution under the many criminal statutes and authorities listed in the Appendix to DHS's *Cybersecurity Strategy*. Nothing could be more cost-effective than having the government take the lead when a cyber event occurs on the project.

4. **Consequence Mitigation**

DHS rightly focuses consequence mitigation on an *effective* response. In other words, simply reporting an incident to authorities may do little to mitigate another attack on your network. Hiring a consultant, after the fact, to safeguard against more cyber events will probably be far more costly than if you hired the same consultant to implement shields before the project. Failing to

investigate and report the smaller events will hardly prevent the larger ones and may only make them worse. It makes more business and legal sense to respond immediately, fully and effectively to minimize the consequences of another event or to try and prevent another one entirely.

5. **Enable Cybersecurity Outcomes**

You have to build a culture of cyber awareness and accountability from the ground up to enable the best outcomes. There should also be punitive consequences for grossly negligent and completely preventable breaches. At one extreme, breaching cybersecurity in the U.S. military could be a court martial offense. In the private sector, on the other hand, a contractor can certainly condition a project manager's job upon his duty to follow the company's cybersecurity protocols. The contract documents for the project can also include an overall commitment to cybersecurity in the same way the contract documents commit everyone to safety and workmanship standards.

Enabling the best cybersecurity outcomes also requires a certain amount of practicality. You may find it impossible, for instance, to stop a twenty-something laborer from using his personal smart phone on the project to upload and text photos to a project manager's company device. But you can help that same laborer understand how doing so may compromise the company network, and why you will provide him with the tools to follow more secure alternative measures instead. The "five pillars" are, in the end, helpful guidelines to implementing a comprehensive cybersecurity plan for all involved, and the "five pillars" provide a sensible backdrop for achieving practical cybersecurity goals for contractors, designers and owners alike.