A white paper from The Net Effect, L.L.C.

Securing the Supply Chain Through Resilience

by Glenda R. Snodgrass
(grs@theneteffect.com)
https://theneteffect.com
(251) 433-0196

With the advent of the Internet of Things (IoT) and Cyber Physical Systems (CPS), technology has become an integral part of the international supply chain. Without proper security, however, this technology has become the soft underbelly of our industrial and transportation systems – easy to attack and inflict serious wounds. To correct this situation, we need to face three hard truths:

Hard Truth #1

We need to stop thinking of cyber security as a cost hurting the bottom line.

Many organizations consider technology that improves processes or increases sales to be investments, while cyber security products and services are expenses (to be avoided if at all possible).

In "Deliver Uncompromised," the MITRE Corporation states that security should be considered a profit center for the acquisition of new business. That's a radical thought! But consider this: Your customers want to know that you will be there for them. They want to know that your systems will not go down for hours, days or even weeks when a cyber attack occurs. If you are not available to your customers, they will find a replacement that is available – and they may not come back when you're up again.

Many companies are starting to require cyber security assurances in writing from their suppliers. From simple questionnaires to signed attestations of compliance with a given standard or framework and even third-party certifications, cyber security is becoming a factor in vendor selection. Your security posture can help you win jobs against your competitors – or the lack thereof may help your competitors win jobs against you.

Hard Truth #2

Much of the technology used in our supply chain today was developed without consideration for security.

Have you read about security researchers taking over a Jeep from its driver? What about traffic light systems that failed when attacked by ransomware? Vending machines infected with malware took down the network of a British university. A casino suffered a data breach because of aquarium equipment that was used to infiltrate the casino's data network.

The stories are both abundant and ludicrous, yet follow a central theme: too many IoT and CPS products today are rushed to market with loads of "features" but no security.
This is problematic because security is much more difficult to add on than it is to include in the design stage. We are left with the task of securing systems built on insecure foundations.

Hard Truth #3

Our reliance on technology has caused us to abandon analog options, creating single points of failure.
In 2017, more than 20 ships in the Black Sea were hit with a GPS attack that disrupted their navigational systems, incorrectly showing the ships' positions in places they were not (and couldn't possibly be). Just as nearly everyone under the age of 30 has never used a rotary

dial phone, many sailors today don't know how to navigate by the stars. If the GPS goes down, they are literally lost. This is why the US Naval Academy reinstituted the instruction of celestial navigation in 2015.

When we rely too heavily on technology, we create single points of failure where our systems will break down when the technology fails.

The Answer? Building Resilience

Dictionary.com defines resilience as *"the ability to recover."*

The NIST Cybersecurity Framework defines five "core functions" in an effective information security program: Identify, Protect, Detect, Respond, Recover. Many organizations do a half-decent job with Identify, dedicate most of their resources to Protect, and stop there.

Remember, it's no longer a matter of "if" you will suffer a cyber incident, but rather "when." Your organization's ability to Detect an attack when it occurs, Respond appropriately and Recover from the attack is critical to its future viability.

How does one build resilience? The exact recipe will be different for every organization, but many ingredients are common:

- Choose the right systems for the job (Was security a design consideration?)
- Segmentations to isolate vulnerable IoT and CPS devices from other network systems
- Redundant systems
- Good data backups
- Manual options for technical processes
- Cooperation and communication between organizational units
- A written incident response plan
- Table top exercises to practice, test and improve the plan

An experienced team of consultants can help build resilience in your organization. Contact us to find out more.

The Net Effect, LLC
Your security is our business

Post Office Box 885
Mobile, Alabama 36601-0885 (US)
phone: +1 (251) 433-0196
https://www.theneteffect.com

The Net Effect, L.L.C. is an independent consulting firm providing information security consulting services to commercial, non-profit and governmental organizations. The company was founded in Mobile, Alabama in 1996 and has worked with businesses across the US, in Canada and in Europe.

Glenda R. Snodgrass (CCP), President and lead consultant for The Net Effect, specializes in information security training and compliance. She has extensive experience teaching and training security awareness and compliance requirements. She has conducted numerous workshops covering PCI DSS, GLBA, FAR 52.204-21, DFARS 252.204-7012, NIST 800-171, NIST CSF and CMMC. Her public speaking includes regional and national conferences of multiple organizations for security professionals. Glenda holds a B.A. from the University of South Alabama (1986) and a maîtrise from Université de Paris I - Panthéon-Sorbonne in Paris, France (1989).