Cybersecurity for Manufacturers: Are You Ready for the 12/31/17 Deadline?

Martha Daniel, Founder, President and Chief Executive Officer, Cytellix and Information Management Resources, Inc. (IMRI)

Moderator: Emily Tjaden Sylvester, AMP SoCal

AMP SoCal Webinar Series: Episode 3
June 8, 2017; 10:00 a.m. – 10:30 a.m.
About AMP SoCal

- The Advanced Manufacturing Partnership for Southern California (AMP SoCal) is a collaboration of more than 135 different organizations.

- Its goal is to strengthen the industrial ecosystem for aerospace and defense manufacturers.

-AMP SoCal is led by the University of Southern California (USC) Sol Price School of Public Policy - USC Center for Economic Development.

-AMP SoCal supports the aerospace and defense manufacturing industry within the 10-county Southern California region.
Logistics

• All audio will stream through your computer speakers.

• Please submit your questions anytime throughout the presentation in the chat box, located on the bottom of your screen.

• Webinar recording and slides are posted within one week of the event.

ampsocal.usc.edu/webinars
Today’s Speaker

Martha Daniel,
Founder, President and Chief Executive Officer of Cytellix and its parent company, Information Management Resources, Inc. (IMRI)

- [www.cytellix.com](http://www.cytellix.com)
- [www.imri.com](http://www.imri.com)
Cyber Security Readiness for Manufacturing by 12/31/17:
NIST SP 800-171 Compliance to meet DFARS 252.204.7012 Regulations

www.cytellix.com

Cytellix, Cyber Security Division of IMRI | Aliso Viejo, CA

Copyright © 2017 IMRI. All rights reserved. Proprietary Information
Today’s Agenda

- Introduction
- Cybersecurity Preparedness
- Industry Standards driving Compliance
- What should be done
- Common questions
- Q&A
Who am I?

Martha Daniel, Founder, CEO & President of Information Management Resources, Inc. a 25 year old company that provides cybersecurity, program management, technology and engineering services to the federal government & private sector

IMRI, Delivering comprehensive IT and engineering solutions since 1992

Successfully delivered over $185 Million in technology contracts. An for over 9 years, IMRI has support Cyber Security programs for the U. S. Federal Government nationally and internationally. Supporting over 1500 networks with 7M endpoints

Cytellix, is the commercial compliance based cybersecurity division of IMRI

Focused on helping small manufacturers meet new Federal Supply chain compliance guidelines around cyber security readiness

Partnered with Manufacturing Extension Partnerships (MEP) around the U.S.
Commercial Market

Managed Cybersecurity Service

Providing a turnkey, affordable, comprehensive solution to help the small and medium business meet Cyber requirements that includes:

- CSET Assessment management & report
  Scaled to meet NIST 800-171 requirements
- Network scan and real-time assessment & report
- Gap Analysis & Assessment of 14 controls & report
- Plan of Action & Milestones
- Continuous network asset monitoring
- Remediation – best practices & practical implementation

Federal Market

Cybersecurity Expertise

For over 9 years IMRI has been providing Cybersecurity support and services to U.S government agencies:

- U.S. Cyber Command
- Defense Information Systems Agency
- Office - Secretary of Defense
- U.S. Strategic Command
- U.S. Southern Command
- U.S. European Command
- U.S. Northern Command
- U.S. Central Command
- U.S. Army Network Enterprise
- U.S. Navy Naval Air systems Command
- U.S. Marine Corps
- Defense Threat Reduction Agency
- Missile Defense Agency

- Cybersecurity services are protecting over 1500 networks, 7 million devices

Confidential & Proprietary © 2017 IMRI

Translating business needs into technology solutions
Quick Survey...

- Raise your hand if...(Keep them up please)
  - You or someone you know has had their personal credit card or identity stolen
  - Your company or a company you know has been hacked
  - Your company or a company you know has been hit with ransomware
  - Your company or a company you know has paid ransomware…

You are likely running out of hands and your arms are getting tired.
Cyber Attacks on the rise!

Attacks are becoming common place. Hacking is a fact of life.
Cyber Attacks on the rise!

60% of SMB cybercrime victims go out of business within 6 months of attack (NCSA)

50% of all surveyed in 2014 reported being victims of cyber attacks. (National SBA)

70% of all targeted attacks struck small to mid-sized organizations in 2016 (SMB Group)

50% of small and midsized businesses have fallen victim to ransomware

48% of those paid a ransom (2017 Ponemon Institute)

79% percent of small businesses do not have an incident response plan. Without one, you may never be able to fully recover when a cybersecurity incident becomes a reality.
Who is Attacking?

Nation States

Hacktivists

Organized Crime
Manufacturer in NJ: Put out RFP for components. Provided information about its products to bidders. Later found out it was being hacked. FBI found out that a Chinese company which bid on the same RFP and lost the bid hacked the other company’s systems and stole their IP, then reproduced their product for sale on Chinese black market.
US Reported Cyber Incidents by Critical Infrastructure Sector. (Source: Department of Homeland Security 2015.)
Regulatory Mandate for Cybersecurity Compliance

Safeguarding Unclassified Controlled Technical Information

- DFAR’s 252.204-7012
- Compliance 12/31/17
- NIST SP 800-171
- Cyber Security Evaluation Tool (CSET®)

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

Confidential & Proprietary © 2017 IMRI

Translating business needs into technology solutions
Cybersecurity for Manufacturers

- All contractors must implement full compliance no later than December 31, 2017
- Contractors must notify the DoD, of any security gaps, within 30-days of any contract award
- Adequate security is defined as a minimum in NIST 800-171 with the 14 controls (to protect controlled, unclassified data):
  - Access Control
  - Awareness and Training
  - Audit & Accountability
  - Configuration Management
  - Identification & Authentication
  - Incident Response
  - Maintenance
  - Media Protection
  - Personnel Security
  - Physical Protection
  - Risk Assessment
  - Security Assessment
  - System & Com Protections
  - System & Info Integrity
OUSD Announced **DFARS 252.204.7012**: “Compliance with safeguarding covered defense in information controls” (Oct 2016)

**DFARS** points to **NIST SP800-171** for guidelines around Controlled Unclassified Information in Non Federal Info Systems & Orgs

- DoD contractors including small businesses must adhere to two basic cybersecurity requirements
  1. **Must provide adequate** security for information that resides in or transits through internal unclassified systems
  2. **Must rapidly report** cyber incidents and cooperate with the DoD to respond to security incidents
What Do You Need to Do?

**Regulatory Needs for Compliance:**

- CSET completed – (DHS Self Assessment tool)
- GAP analysis completed with a plan of action for remediation and priority list defined
- Have a continuous improvement and awareness program in place (continuous monitoring)
- Prepare for notification to your contractor should you be hacked

<table>
<thead>
<tr>
<th>Internal Strains</th>
<th>Outsource Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Knowledge of regulation</td>
<td>• Compliance based managed cyber services</td>
</tr>
<tr>
<td>• Cybersecurity skills</td>
<td>• Cybersecurity experts</td>
</tr>
<tr>
<td>• Understand the changes needed for a secure network (DELAYS)</td>
<td>• Technical expertise to understand the gaps</td>
</tr>
<tr>
<td>• Create an accurate detailed remediation plan</td>
<td>• Low friction to avoid disruption of business</td>
</tr>
<tr>
<td>• Dedicated time</td>
<td>• Assurance done right</td>
</tr>
<tr>
<td>• Consistent time invested in ongoing efforts</td>
<td>• Managed cyber services</td>
</tr>
<tr>
<td>• Ensure dedicated resources &amp; skills</td>
<td>• Cost effective</td>
</tr>
<tr>
<td>• Drive urgency</td>
<td>• Cyber expertise (less of a headache)</td>
</tr>
<tr>
<td>• Mitigate risks</td>
<td>• Mitigate risks</td>
</tr>
<tr>
<td>• Ability to identify: what, how, when, why &amp; docs.</td>
<td>• Managed documentation</td>
</tr>
<tr>
<td>• Explanations under “duress”</td>
<td>• Proactive</td>
</tr>
<tr>
<td></td>
<td>• Ease of reporting</td>
</tr>
<tr>
<td></td>
<td>• Discovery is easier</td>
</tr>
</tbody>
</table>
What if....Manufacturer Questions

- What skills are need to accomplish this?
  - Outsource or become an expert

- Are there services that provide a complete documentation and improvement program?
  - Yes, look for a managed service provider that can take you through the entire process

- What happens if the supplier doesn’t do this?
  - You will **LOSE** your current contracts
  - You will **NOT** be awarded new contracts
  - You will be Hacked, no question (not if but when)

- What happens if my cyber results are poor?
  - It is very important to provide accurate results and plans.
  - Build a plan of action to show remediation steps for improvement
  - Prevent cyber incidents and report according to guidance – see first bullet
December 31, 2017

- CSET must be complete – *(In-house or outsourced)*
  - POAM and GAP Analysis – **COMPLETED**

- Remediation Plan – **FIX IT PLAN** – you have 30 days prior to contract award. It is required that you have an continuous ongoing monitoring of the plan to remain in compliance

- Need Assistance? Don’t wait or hesitate

Contact us at – **CYTELLIX**  [WWW.CYTELLIX.COM](http://WWW.CYTELLIX.COM)
Cybellix Cybersecurity
Tips and Tricks

- Never open email from unknown senders
- Right click on email addresses to verify sender’s domain is legitimate, prior to opening an email message.
- When in doubt about an email and its intentions, call the sender to verify.
- Use two step verification / authentications
- If it’s being offered for free, it’s never free
- Use antimalware and antivirus products vs nothing
- Always update security when requested by legitimate publishers
- Back-up your data, use multiple places/locations.
- Back up your data offline when possible
- Do not download applications from unknown publishers or sites
- Never share USB keys/drives
- Do not open attachments in email messages from suspicious senders – verify sender and intentions
- Using mobile devices for browsing is just as risky as laptops for discovering malware and virus’s
- Check what ports are open on your network and their behaviors
- Segment your network for guest and internal users
- Public Wi-Fi networks are very risky for data protection on your devices – use a VPN
- Use a secure password manager for all your unique passwords
- Never us the same password 2x
- Physical spying takes place as much as digital spying, watch who is looking over your shoulder.
- No one is protected from being hacked, you are, will and have been hacked!
- Set strong privacy setting on your devices – you don’t want to overshare

- Java script in your browser is insecure, disable it!
- Always ask yourself questions about communications sent to you, be suspicious is the best practice.
- Use the best browser available from a security perspective, stay aware of exploits of browsers.
- Patch, patch, patch!
- Pay attention to mobile app permissions and access, some will access very private, personal and proprietary information you want to remain confidential.
- Clean up (delete) apps you don’t use
- Use device passwords to lock and encrypt the data wherever possible – losing a device is painful enough!
- Never leave devices set to default
- Change Wi-Fi passwords often and never repeat them
- Don’t use names, birthdates, and phone numbers as passwords – be unique and complex
- Social media has risks associated with personal information – don’t feed the bad guys information they can use against you.
- Inventory your devices and their IP addresses on your network
- Remove any devices that are end-of-life from their manufacturer from your network – they are attack points
- Log-out of services like banking when your done with your business.
- Don’t store UID/PW in cookies on devices, just don’t do it
- IoT is pretty cool, but, make sure you manage these IoT devices with the same care as your computer.
Cytellix is the compliance based cyber security managed service provider with a focus on small-and-medium size businesses. We specialize in comprehensive cyber assessments, network intelligence, behavioral analytics, remediation and security services. A division of Information Management Resources, Inc. (IMRI), the Cytellix team of experts manage millions of IP addresses for organizations of every size in a wide range of data-rich industries—including municipalities, manufacturing, finance, banking, law, education, healthcare and biotech—with best-in-class managed services.

Visit us at cytellix.com

Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations
Download CSET Cybersecurity Evaluation Tool
https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET
NEXT WEBINAR:
Clean Energy Smart Manufacturing Innovation Institute (CESMII)

Speaker: Gregg Profozich, Interim Director, CESMII CA Regional Manufacturing Center

AMP SoCal Webinar Series: Episode 4
July 13, 2017; 10:00 a.m. – 10:30 a.m.

REGISTER: ampsocal.usc.edu