The State Of Security In SLED Markets

George Pashardis – RVP Sales, ePlus Technology, Inc
Paul J. Karch – Founder & Chairman, Gardant Global
Carmine Taglialatela – Principal & Founder, Oak Hill Farm Group, LLC
What is Cybersecurity?

What are the Risks & why is it important?

What are the Challenges in defending?

What is a Cybersecurity Framework?

How do I defend my agency/school?

Questions
Recent Attacks!

Cyberattack disrupts school testing

Carly Q. Romano (Cherry Hill, N.J.) Courier-Post 7:53 p.m. EDT March 24, 2015

SWEDESBOG, N.J. — A controversial statewide test was interrupted for two days by a cyberattack on Swedesboro-Woolwich Schools' network, according to district officials.

The Web-based testing — Partnership for Assessment of Readiness for College and Careers (PARCC) — is expected to result in four district elementary schools' programs held in districts' computer exchange for 500 bitcoins, a cryptocurrency.

The Gloucester County Prosecutor's Office is now investigating the network hijacking.

Cloquet School District's computer network shutdown by malware

By Alec Bochniak
March 17, 2016
Updated Mar 17, 2016 at 10:15 PM CST

Cloquet MN (NNCNOW.com) — Cloquet schools were closed for the second straight day. But today, it wasn't because of the snow.

The school's computer system took a major hit by a virus.

The virus infiltrated the Cloquet School System and shut down five different schools.

NNCNOW Click here to subscribe to our daily newsletter.

The IT Department says it was a malware virus called ransomware.

"I have never experienced anything like this. Technology is a wonderful tool for education. But when it isn't working, it poses a serious challenge," said Kim Scarbrough, Cloquet Superintendent.

XChange® SLED

SC school district pays nearly $10k to 'ransomware' hackers

By Andrew Stelzer
Published March 3, 2016, 9:03 am | Updated March 3, 2016, 10:31 am

CONWAY, SC (WBTW) — Horry County Schools in South Carolina paid nearly $10,000 to hackers who attacked the district's network, district spokesperson Teal Harding confirmed on Monday.

The hackers locked files across the district's network in February and required a ransom to unlock them. Similar attacks, with a virus known as ransomware, have hit networks across the country.
State CIO Priorities for 2016
November 10, 2015

A. Priority Strategies, Management Processes and Solutions
Top 10 Final Ranking

1. **Security and Risk Management**: governance, budget and resource requirements, security frameworks, data protection, training and awareness, insider threats, third party security practices as outsourcing increases, determining what constitutes "due care" or "reasonable"

2. **Cloud Services**: cloud strategy, proper selection of service and deployment models, scalable and elastic IT-enabled capabilities provided "as a service" using Internet technologies, governance, service management, service catalogs, platform, infrastructure, security, privacy, data ownership

3. **Consolidation/Optimization**: centralizing, consolidating services, operations, resources, infrastructure, data centers, communications and marketing "enterprise" thinking, identifying and dealing with barriers

4. **Business Intelligence and Data Analytics**: applying BI/BA within the enterprise, communicating the value, building expertise, delivering shared services, exploring big data, data analytics

5. **Legacy Modernization**: enhancing, renovating, replacing, legacy platforms and applications, business process improvement

---

**Enterprise Vision and Roadmap for IT**: vision and roadmap for IT governance

---
What is Cybersecurity

“Cybersecurity refers to preventative methods used to protect information from being stolen, compromised or attacked. It requires an understanding of potential information threats, such as viruses and other malicious code. Cybersecurity strategies include identity management, risk management and incident management.

Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. A range of traditional crimes are now being perpetrated through cyberspace. In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become an important security mission.”
The Risks

- Ransomware – Schools/Government are being targeted
- Malware – 1M variants per day
- DDOS – Buy online for a few $$$
- Spear Phishing – the trust threat
- Website Defacement – ISIS & others
- Identity/Data Theft – Children have a 51% higher theft attack rate than adults
Important...Why? Impact to Digital Learning/Privacy

- Google for Education
- Office 365
- PARCC Testing in 22 States
- 1 to 1 computing
- BYOD
- Student Information System
- Business systems – Benefits, payroll, pensions
Challenges in Defending the infrastructure

- It’s complicated & we don’t know where to start - need to access the current posture
- It’s a living breathing thing that’s always changing – 100% protection is not possible
- The Human Factor – people are the weakest link and “trust their IT”
- Technologies use point products & don’t correlate together – Huge gaps in defense
- People confuse compliance with safety – you can’t just “check boxes”
- Don’t have the trained staff to deal with security alerts – need actionable intelligence
- We think we’re secure because nothing has happened – don’t have visibility
- School District leaders are not educated or informed on the risks – Mitigate Risk
- Behavior – Almost always reactive in nature – need to change culture to proactive
What is Cybersecurity Framework

- NIST – National Institute of Standards and Technology
- The framework enables organizations to apply the principles & best practices of risk management to improving the security and resilience of critical infrastructure. It provides organization & structure to today’s multiple approaches to cybersecurity by assembling standards, guidelines and practices that are working effectively in industry today.
- The framework is not a one-size fits all approach to managing cybersecurity risk. Each entity may have it’s own unique risk – different threats, different vulnerabilities & different risk tolerances. The framework will continue to be updated and improved.
What is Cybersecurity Framework - Functions

- **Identify** – Develop understanding to manage risk to systems, assets, data, capabilities
- **Protect** – Develop/Implement safeguards to ensure delivery of services
- **Detect** - Develop/Implement to identify a cyber event
- **Respond** - Develop/Implement to take action of a cyber event
- **Recover** - Develop/Implement to maintain or restore services after cyber event
How do I defend – create the process

- Stop asking if or when and start asking “How do I respond?”
- IT Health Check – assess the current approach & create a risk profile
- Security is a process, not a product – all parties in organization have a role
- Establish the Cybersecurity framework – improve your posture & risk
- Create an adaptive defensive strategy – Technology, intelligence, expertise
- Adopt a platform approach – systems can correlate for actionable intel
- Who can I partner with to help manage risk? K12 btw…can’t do it alone
- Cybersecurity education & incident response plan
- Red Team testing – challenges an organization to improve it’s effectiveness
Cybersecurity Technology Partners

![Partner Logos]