STEPS NONPROFITS CAN TAKE TO BOLSTER CYBERSECURITY

Paul Centanni
Senior Solutions Architect

pcentanni@convergeone.com
518-406-0916

Connecting Solutions, Delivering Outcomes.

ConvergeOne

CYBERSECURITY 500
WORLD'S HOTTEST SECURITY COMPANIES

THE NONPROFIT'S FOCUS ON CYBERSECURITY

People

> Prioritize Information Security as foundational
> Identify who's Responsible, Accountable, Consulted and Informed (RACI)
> Communication, Awareness and Training

Process

> Governance and Cybersecurity frameworks
> Audit and Business alignment

Technology/Platform

> Effective, adjoining toolsets to protect data confidentiality, integrity and availability (CIA)

PEOPLE – TRAINING IS KEY

Email is the number 1 attack vector for malware (94%).*

- It is important to train your users to recognize a phishing email or a scam phone call.
- A robust, all-employee phishing simulation strategy is highly recommended to combat the #1 attack vector
- Mandatory and periodic security awareness training is highly recommended for all employees
- Other social engineering simulations are also important
- Also recommended are reminders such as posters and visual aids

*Verizon 2019 Data Breach Investigations Report - https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

PEOPLE - DEDICATED ISO/CISO

- A dedicated CISO or vCISO will align technology platforms to information security policies and processes
- What are you protecting? What are your compliance obligations? A CISO will wrap his head around things like this
- A CISO can provide senior leaders with executive risk assessment insight to gain support for key initiatives
- Leadership is the most important factor to influence awareness and mindset

PEOPLE - 24X7 ACTIVE MONITORING

Over 1 million unfilled position in cybersecurity. Said to reach 3.5 million by 2021*

- Who's actively monitoring your environment when no one is there?
- A 24x7 monitoring service with actionable intelligence and notification SLAs may be beneficial to ensure information flowing through the network is being watched around the clock
- Experts included

* Cybersecurity Ventures https://cybersecurityventures.com/jobs/

PROCESS – IMPLEMENT A CYBERSECURITY FRAMEWORK (CSF)

- A cybersecurity framework will be your guide to not missing anything in your security program

- Fully implementing the **NIST 800-53** or **CIS Top 20** controls is recommended as a CSF

- Assess against your CSF on an annual basis with Gap Analysis and Maturity Mapping

PROCESS - ASSESSMENTS

- Regular assessments will let you know where you stand and help you optimize
- Perform a risk assessment. Inventory your assets and measure associated risks to them
- Perform a risk assessment annually
- Periodic vulnerability assessments followed by penetration tests are recommended. This will expose weak spots and allow for recurring optimization
- Quarterly vulnerability and penetration tests should be performed

PROCESS – BACK UPS AND DISASTER RECOVERY

- Have good backups that are air gapped from the network in case recovery from a Ransomware or similar attack is required
- Backup all critical systems, VM images, and end user devices
- Maintain 3 copies: snapshot, backup disk, and offline (air gapped)
- Test restore periodically
- Have a good DR plan in place so you can recover from a major outage
- Have a DR plan documented that is practiced

PROCESS – RECURRING OPTIMIZATION

- Continually optimize based on feedback you receive from the assessments, CSF gap analysis, etc.
- Use “lessons learned” for optimization
- Conducting regular optimization of security platforms to avoid system stagnancy is recommended to maintain a high level of efficacy
- Recommend creating a scheduled optimization schema

PROCESS – INCIDENT RESPONSE

- Be prepared to respond well in the event that something does happen
- Recommend structuring a comprehensive Incident Response retainer with 1 Hour response SLA or better
- Perform semi-annual table top tests with lessons learned

TECHNOLOGY – NEXT GEN PROTECTIONS

Traditional tools are no longer effective

- Strongly recommend incorporating next generation feature sets into all perimeter security measures and firewalls (IPS, anti-malware, and content filtering with a quality security intel feed)
- DNS layer security to help protect internet perimeter
- Strongly recommend protecting endpoints with a modern endpoint solution capable of identifying modern threats (AI based)
- Next generation firewalling is recommended between data center and users to limit trust boundaries

TECHNOLOGY – MULTIFACTOR AUTHENTICATION

- Passwords can easily be stolen, lost, given away, or cracked
- Multiple Factor Authentication (MFA) is highly recommended for all critical applications
- Local apps, cloud apps, remote access, etc.
- Consider modern solutions that enable posturing as part of the authentication process

TECHNOLOGY – 24X7 MONITORING

- Managed Security Services are often ideal due to the significant cost to self-operate a 24x7 monitoring environment in technology and people but can be done in-house

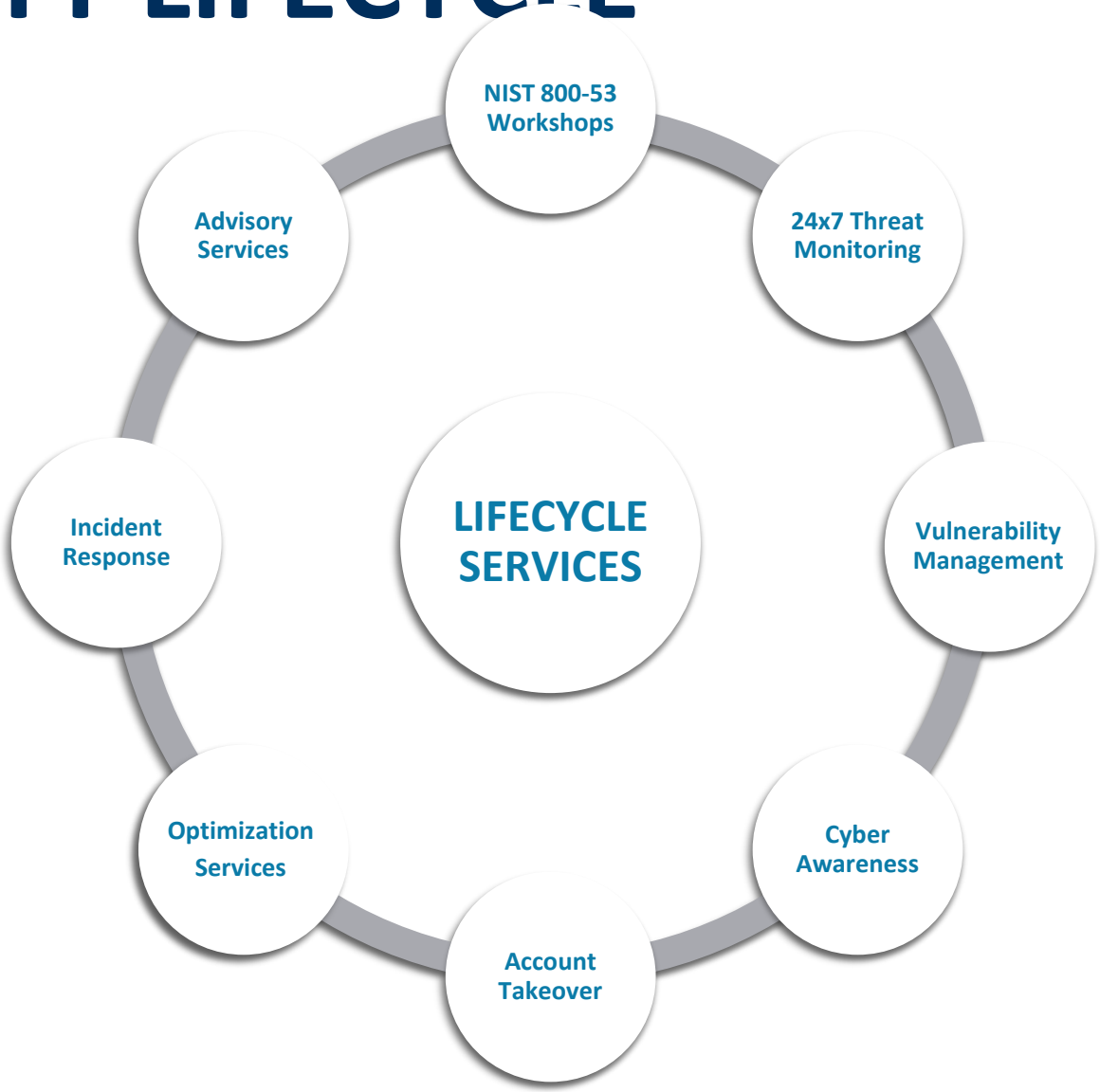
- If going to self monitor at minimum need to know about Indicators of Compromise

- Mature threat correlation environments provide 24x7 monitoring of ingress and egress traffic flows in addition to active monitoring and storage of logs

BUILD A CYBER SECURITY LIFECYCLE

Cybersecurity Lifecycle Includes:

- NIST 800-53 Framework Assessment
- 24x7 Threat Monitoring and Intelligence
- Vulnerability Management Program
- Cyber Awareness Program
- Account Takeover Monitoring
- Optimization Services
- Incident Response
- Advisory Services (vCISO)



THANK YOU

Paul Centanni

Senior Solutions Architect at ConvergeOne

pcentanni@convergeone.com

(518) 406-0916

PAUL CENTANNI

Paul Centanni is a Senior Solutions Architect working as the cybersecurity lead for the Northeast Region of a national solutions provider. Paul advises enterprise clients on how to best safeguard their environment and valuable data with effective information security. Having worked in the solutions provider space for 25+ years Paul has successfully addressed the security needs of his customers by utilizing people, processes, and technology to secure their infrastructure and valuable data.

Prior to his current role, Paul worked as an engineer and architect with cybersecurity and network infrastructure. During that period Paul spent time designing solutions, advising clients, coordinating teams, and implementing high quality security and network infrastructure solutions.

APPENDIX: DO NOT ALLOW “PERFECT” TO BE THE ENEMY OF “GOOD”

- Perfection rarely happens in security, be “good” and “get better”
- Serious incidents happen in the most security conscious organizations
- Layer – Defense in depth (perimeter, network, host, app, data)
- Limit – Compartmentalize, segregate, limit access and permissions
- Obscure – Hide assets; encrypt widely; consider intelligent deception; if you don’t encrypt, then please at least redact or data mask/subset
- Diversify – Use a variety of techniques; present skinny surface; think like a hacker; present variation
- Simplify – Have a simple set of policies that everyone can understand but remember the four you need:
  - Information Protection, Data Classification, Data Governance, Incident Response and Business Continuity