HEALTHCARE CYBERSECURITY & PRIVACY

Applications and Integrations

Cylidify

Cylidify Background

- Founded 2018; R&D and healthcare focus
- Monty LaRue (Founder) – 25 years experience with technology, security, and leadership
  - 10 years @Microsoft Windows, Xbox, and Trustworthy Computing
  - 6 years @Allscripts
- Tailored, agile approach via consulting and referrals
- “Nothing is ever secure” and there is “no one size fits all” - confidentiality, integrity and ROI are paramount!

Cybersecurity in General

- Pervasive and complex with unprecedented public awareness
- New attacks or derivations of old attacks
  - Agility to stay current with updates and patches is critical
- Attackers are taking creative delivery and monetization approaches leveraging technology advances just like “us”
  - Agile via AI and viral propagation techniques
  - Exploiting differences and gaps in public cloud, mobile, etc.
- Phishing, identity theft, and infrastructure attacks (e.g. DoS, Ransomware, etc.) should be top of mind

Cybersecurity in Healthcare

- Again; “nothing is secure” and there is “no one size fits all”
- New technologies = new challenges (public cloud, mobile, etc.)
  - On-premises prevalent, but many ad-hoc hybrids and integrations
- HIPAA enforcement – fines are real and expensive
- Top of mind:
  - Ransomware (Phishing), Theft, and DoS
  - Development and deployment chain security
  - Solution security: applications + 3rd parties + deployment chain + operations
  - Balance solution security with policies, compliance, and certifications

Whose Line Is It?

"Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals"

- ✓ Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- ✓ The Macarena and Nintendo 64 were also "hot" in 1996 – expect regular tuning and significant changes to align to GDPR and technology advances

HIPAA “Compliance”

- Encrypt data “at rest” and “in motion”
  - Critical for PHI especially *sensitive* data like SSN and health conditions
  - NOT storage level encryption alone (e.g. SAN or Bitlocker)
- Logging of accesses and transactions – required for audits, tracing, and forensics
- Authentication and Authorization (auth:auth) for all capabilities, APIs, and data
- End-to-end consideration of data controls and patient consent

What to do?

- Assess, track, plan, and implement iteratively – crawl, walk, run
- Strike the right balance for *your* business working bottom→top and left→right
- Embrace recognized frameworks like NIST 
- Track dependencies including commercial and open source
- Create process evidence – for compliance, certifications (like HITRUST), audits, and 3rd party assessments

✓ Be careful with deidentified or anonymous data

✓ Be agile and *discrete* in delivery, deployment, and updates

How to do it?

- Build awareness and visibility via training and dashboards
- Track risks via yearly assessments and a risk register
- Executive sponsorship with security/privacy *requirements*
  - Associate security with quality or privacy
- Cybersecurity Incident Response Plan (CSIRP)
- Security Development Lifecycle (SDL) – baked-in vs. bolted-on
  - Threat modeling, static→dynamic testing, etc. 
- Take a balanced, iterative approach: applications→operations, mitigations, defense-in-depth, etc.
- Utilize certifications and 3rd party assessments where *needed*

Red Flags

- Assume “secure” because you haven’t had an incident
- Treat security the same across deployments and configurations
- Utilize “one size fits all” or single-source approaches; second sources and defense-in-depth are key
- Deliver capabilities accruing large security and privacy debt
- Over invest in prevention; must balance with education, monitoring, and response
- Lack of consent checks or data mappings
- Containment of sensitive or confidential information
- Caching of data or session – especially RESTful or mobile

Cylidify Offerings

- Strategic - full range of consulting and services
- Tactical:
  - Assessments
  - Training
  - SDL implementations with threat modeling
  - Remediations: architecture/design, code, compliance, etc.
  - “Virtual” CISO and/or representation of your business
- Visit https://www.Cylidify.com or contact Info@Cylidify.com

Q&A

Thank you!

https://www.cylidify.com/faq

https://www.cylidify.com/blog

Cylidify