# Huntzinger Cyber Security Services

## Prevention, Business Continuity and Remediation

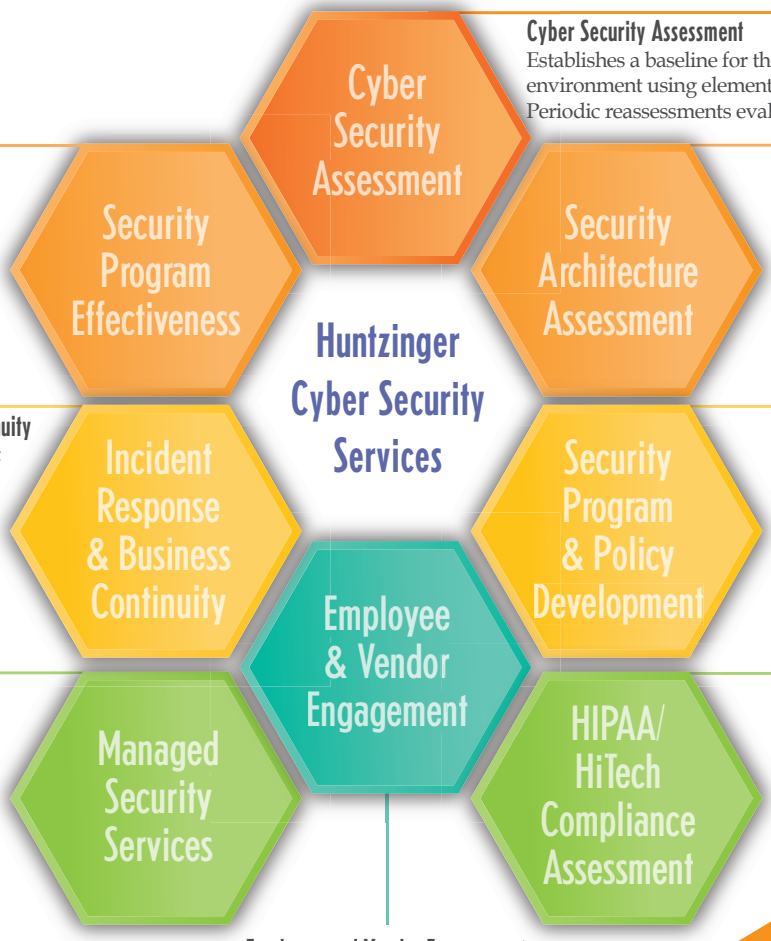
BEST IN KLAS® HIT ADVISORY SERVICES 2020

### Assess Your Organization's Vulnerabilities Precisely and Accurately

The increasing number of computer virus, malware and ransomware attacks on healthcare organizations is forcing executives to reevaluate their information security strategies. Trends indicate that healthcare organizations are particularly at risk, due to the industry's historic underinvestment in information security, the comparatively high "black market" value and exploitation risks of stolen healthcare data, and the fact that most organizations lack a clear understanding of their vulnerabilities.

### Huntzinger's Cyber Security Offerings

Huntzinger is focused solely on the healthcare provider marketplace, and our Cyber Security Services focus on the key elements of the NIST Cyber Security Framework of "Identify, Protect, Defend, Respond and Recover" that are most relevant to healthcare missions and business challenges. We'll develop a comprehensive, yet actionable, roadmap that will guide your Cyber Security Strategy. We also offer customized solutions specific to a focus area, such as ransomware defense and readiness, as part of a full spectrum of Cyber Security service offerings that include:




**Cyber Security Assessment**
Establishes a baseline for the organization's information security environment using elements of the NIST Cyber Security Framework. Periodic reassessments evaluate progress and improvements.

**Security Program Effectiveness**
Test elements of your security program to evaluate effectiveness through services such as penetration testing, recurring vulnerability scanning, hardening assessment, social engineer testing, and policy compliance.

**Security Architecture Assessment**
Delivers a "deep-dive" technical assessment that focuses on the infrastructure to assess the security tools, systems, and technology controls within the environment.

**Incident Response and Business Continuity**
Develop and "road-test" incident response plans. Develop and assess business continuity and disaster recovery plans given the realities of long potential outages or malicious cyber attacks.

**Security Program & Policy Development**
Improves the design of security program and associated management framework inclusive of policies, governance, technical remediation, education and program stability over time.

**Managed Security Services**
Through our partner you have access to continuous monitoring and expert analysis via remote operations centers to detect and respond to threats and vulnerabilities. Mitigation, prevention, and response assistance protect your critical assets and data.

**HIPAA/HiTech Compliance Assessment**
Review current HIPAA and HiTech policies, identify gaps or vulnerabilities and develop a remediation plan.

**Employee and Vendor Engagement**
Security awareness training and testing, simulated phishing, vendor security reviews and management, evaluating third-party security controls, and vendor HIPAA compliance reviews.

HUNTZINGER

Huntzinger offers a full spectrum of advanced Cyber Security capabilities that include the following featured offerings:

## Cyber Security Assessment – Your First Step Toward Reducing Vulnerabilities

Huntzinger's Cyber Security Assessment creates a baseline to evaluate an organization's vulnerabilities and the overall maturity of its security program. Focusing on key elements of the NIST Cyber Security Framework, Huntzinger conducts an assessment of an organization's Security environment that includes, but is not limited to:

- High-level governance, policies and related documentation
- Staff onboarding and exit procedures, awareness training, and policy adherence
- System access control, vulnerability patching and backup procedures
- Infrastructure, network, mobile device, firewall and perimeter security
- Application development and third-party/cloud application provider security practices
- Email protection, data transmission security, and data loss prevention
- Threat monitoring capabilities, incident response planning and protocols
- *Huntzinger also provides a phased actionable roadmap segmented in 90-day, 180-day and 180-day-plus intervals.*

## Customized Ransomware Threat Assessment

Optional services include customized solution offerings such as ransomware threat assessments:

- Advanced-threat end-point hardening assessment inclusive of testing and evaluation of hardening standards against known ransomware attacks.
- Test simulated malware, determining if controls can prevent it from executing, and determining if common command-and-control vectors may be available.
- Ransomware/malware-focused security architecture assessment, including technical architecture review of perimeter, workstation, and laptop/mobile security standards and controls.
- Social engineering awareness and susceptibility assessment. Includes email phishing testing, as well as evaluating the development and use of end-user awareness training materials.
- Detection and evaluation of known vulnerabilities, ineffective patch management practices, and other related systemic gaps in the client environment that are vulnerable to ransomware.

## Know the Risks

- In the first half of 2016, 88% of ransomware detected by one security vendor targeted healthcare. This is due in part to the willingness by the victims to pay the ransom, despite the perils of doing so, when patient care has been put at risk.[1]
- 87% of organizations indicated that information security had increased as a business priority in the HIMSS 2015 Cyber Security Survey.[2]
- 90% of organizations had at least one security breach in the previous year, according to a recent study.[3]
- Many organizations lack the funds and resources to protect patient data and are unprepared to meet the changing cyber threat environment, a study revealed.[3]

1. Solutionary's Security Engineering Research Team Quarterly Threat Report for Q2 2016.
2. 2015 HIMSS Cybersecurity Survey | Full Report. (2015, June 30). Retrieved April 13, 2016, from http://www.himss.org/2015-cybersecurity-survey.
3. Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data [PDF]. (2015, May). Ponemon Institute LLC.

## Why Huntzinger?

- **We Know Security —** Huntzinger and its partner have broad and deep security knowledge and expertise, designed to provide both immediate and sustained impact.
- **Healthcare Experience —** Healthcare is our sole focus. Our consultants have worked at major hospital systems and other healthcare providers, many as CISOs, CIOs/CTOs/VPs in technology and more. We have been in your shoes, and beyond that our talents and collective experience have been enriched through many, and diverse, client engagements.
- **Highest Quality Delivery —** Huntzinger has a strong recruitment and evaluation process for our resources, ensuring that we match consultants to your organization's culture and specific role requirements, who then produce and deliver quality results on your behalf.
- **Strong Partnerships —** Huntzinger has relationships with many of the major technology and security providers, and we leverage these relationships to deliver cost-efficient and highly effective solutions.
- **Culture of Performance —** Client feedback, through many and diverse engagements, has consistently been expressed by the terms *Integrity, Commitment, Expertise, Performance and Results* — which, by design, are the keystones of our company culture.

HUNTZINGER™
MANAGEMENT GROUP
Your Healthcare IT Experts

72 Glenmaura National Blvd. | Suite 105 | Moosic, PA 18507
© 2018 The Huntzinger Management Group. All rights reserved.