Risk, Security and Privacy (RSP) Health

Can you afford to take chances with patient data?

online business systems

As your trusted advisors, Online's Risk, Security, and Privacy (RSP) Health team provides clients with a comprehensive administrative, physical, and technical review of their security posture to identify potential vulnerabilities and business risks.

Our RSP Practice offers a suite of services to address the full lifecycle of information security and risk management needs. Drawing from over 20-years of healthcare and cybersecurity expertise, our team uses a proven methodology that is tailored for each client based on their business requirements and risk profile.

Online's team offers the following healthcare information security services:

- > Virtual CISO
- > HIPAA Compliance Assessment
- > HIPAA Security Risk Analysis
- > Ransomware Readiness Analysis
- > Penetration Testing
- > Incident Response Planning
- > Incident Response Tabletop Exercises

Virtual CISO

Competent cybersecurity professionals are in high demand and finding qualified, experienced security professionals is difficult. Whether you are looking for a Chief Information Security Officer (CISO), Security Director, or Security Manager to help lead your organizational security development, an Online Virtual CISO can help.

A Virtual CISO has an in-depth understanding of the ever-changing threat landscape and can effectively analyze and mitigate risk. Our Virtual CISO service is tailored to the unique needs and requirements of each of our clients, while ensuring that customer, patient and organizational data is protected with an effective, and well managed security program.

Our Virtual CISOs become extensions of your leadership teams, participate in strategy meetings and develop policies and key security management documents - all with an eye toward communication, mentorship, and reducing risk.

HIPAA Compliance Assessment

Compliance can be complex and difficult to understand. Healthcare organizations are required to comply with the HIPAA Privacy Rule, Security Rule, HITECH Act, and several other state and federal regulations.

Online's experienced team of assessors have worked closely with regulators such as the HHS Office for Civil Rights (HHS/OCR) to understand their interpretation of these regulations. Our experience with these regulations and security frameworks allow us to recommend "right-sized" security controls that provide a reasonable level of security and compliance, without breaking already-stretched budgets.

HIPAA Security Risk Analysis

The HIPAA Security Rule requires healthcare providers to conduct regular Security Risk Analysis. What constitutes an "accurate and thorough" Risk Analysis according to HHS/OCR can sometimes be difficult to understand.

Online's Threat-Based Risk Analysis goes beyond adherence to HIPAA Security Rule, featuring proprietary advanced tooling and a methodology designed to rapidly prioritize realistic threats to critical assets, empowering our clients to focus on the security controls that generate the most immediate long-term value.

Ransomware Readiness Analysis

Are you prepared for a Ransomware attack? Do you have a well defined Ransomware Recovery Plan?

A Ransomware Readiness Analysis helps organizations strengthen their processes and technology to mitigate the threat of Ransomware.

A Ransomware Readiness Analysis provides a quick way for you to:

- Gain visibility to the weaknesses in your environment - technology and processes.
- Understand your current response capabilities.
- Identify areas for improvement in recovery.

Our Ransomware Readiness Analysis is made up of three phases: Discovery, Defense Analysis and Simulations. Our approach allows us to assess your current state of readiness and develop a ransomware prevention playbook that will ensure you are prepared for ransomware attacks.

Penetration Testing

Penetration Testing assesses your organizations' ability to hold up against an attack and detect where the weak points are in your security controls.

Our Penetration Testing services provide your business with an in-depth technical review of your current security posture by providing a comprehensive analysis of vulnerabilities, their exploitability, associated business risk and most importantly, how to fix them. Healthcare organizations often have different Penetration Testing requirements depending on what they are trying to achieve. Some need to assess how an attacker, with little to no information about your environment, may be able to circumvent controls or otherwise gain unauthorized access. Others want to better understand insider threat – an employee or contractor – and how they may use additional information to gain unauthorized access.

Our team has experience across an array of environments including internal and external networks, wireless networks, applications, application programming interfaces (APIs), mobile apps, and cloud environments and can work with you to design the level of penetration testing appropriate for your business needs,

Incident Response Planning

Online recognizes every organization has a responsibility to protect their most critical assets: client information and intellectual property. As such, having an effective Incident Response (IR) plan in place will help you mitigate, and more often, avoid the costly impacts that a security breach can have on a business.

Our RSP Health team takes an interactive and proactive approach to IR planning: we collaborate with your team to gain a clear understanding of your business model to determine what is most critical to you. We identify weak points in the IR plan, such as role confusion, inadequate procedures, or gaps in coverage. We test operational capabilities, identify leadership effectiveness, and examine the ways for your business to prevent, protect from, respond to, recover from, and mitigate cyber-related incidents.

As a Security Advisor we review and provide recommendations for a Disaster Recovery and Incident Response plan that enables you to be more resilient in the event of a cyberattack.

Incident Response Tabletop Exercises

We understand that the COVID-19 pandemic has made businesses, including health centers, more vulnerable to cyber-attacks and has elevated security risks due to increased remote work environments and virtual care models. Incident response and cybersecurity are more important now than ever before, and health centers are tasked with integrating new policies and procedures into their general IT operations.

In order to address these challenges, Online will work with your organization to facilitate workshops to train representatives from medical centers on the concepts of security incident response preparation and execution. We deliver customized workshops using real-life scenarios as learning events, designed to address common threats and how to respond to incidents with a hands-on approach.

FOR MORE INFORMATION

If you have any questions, or would like more information - we would love to hear from you.

Contact
Lee Buttke
Director, RSP Practice
1.612.799.2300
lbuttke@obsglobal.com

online business systems

About Online Business Systems

Online is a leading Digital Transformation and Cybersecurity consultancy. Businesses today are under pressure to transform to remain relevant – at the same time, there is unprecedented opportunity to innovate and achieve incredible things never seen before – securely.We combine the best technology, business, and security practices, and lead Clients through the transformation process.