

healthcare report

VICTOR O. SCHINNERER & COMPANY, INC.

Information and Risk Management Ideas for Healthcare Professionals

PROTECTING HOSPITALS AND HEALTHCARE OPERATIONS FROM CYBER LIABILITY

WITH the growth of electronic record-keeping and digital communications, it is all too common that businesses underestimate their data security breach risks.

Hospitals and other healthcare operations amass a great deal of confidential information about their employees, patients, procedures, research, and financial status. Most of this information is collected, processed, and stored on computers and transmitted digitally to other computers across networks both internal and external. Exposure to cyber liability arises in any communication or data storage system and can vary from the obvious dangers of transmitting and storing sensitive information to the less evident risks of maintaining a website. Cyber liability risks include the failure to prevent unauthorized access to computer systems by a third party or an unauthorized employee, the disclosure of or misuse of confidential information, and the violation of privacy laws.

Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement. The increasing use of technology creates an increasing vulnerability to cyber security threats, any of which can result in significant out-of-pocket and reputational costs.

Any breach or concern that a breach occurred could mean a potential loss of confidence in the organization by those that rely on the hospital or healthcare entity for services or those who interact with it on a business-to-business basis.

Healthcare Industry Has Specific Risks

Protecting the privacy of patients is basic to the operations of any healthcare facility. That privacy can be compromised; personal information can be obtained in many ways and used inappropriately. The risks are not only that the information will be damaged, stolen, or misused; the actual or implied theft of improperly protected electronic data also can result in an extortion threat. The costs and distraction of a hacker's extortion demand that threatens to shut down an entity's system or to expose confidential information can be enormous. In addition to the direct costs related to the extortion demand, a facility can have major expenses, including those for the required notification of patients related to the real or threatened release of their identity information. Many states require companies to notify all of their customers if a breach is even suspected and to take all necessary actions to correct any breach.

The integrity of computer systems can be breached even with firewalls, virus

detection, and many other safeguards in place. A breach can even result from a simple mistake such as a misplaced laptop or inadvertently unprotected back-up media. Whether because of internal incompetence, malicious intent, or the desire to extort money, computer systems and the information they hold can be damaged, pilfered, or held hostage. Facilities cannot function without computer systems providing accurate and timely records, controlling systems, and monitoring vital information flows.

Even the use of email is problematic. An email could result in the crash of another party's network or transmit a computer virus or other type of malware. In addition, an email, web file, or blog or forum posting could result in allegations of defamation that are costly to defend. Legal actions can be related to security failure or alleged technology error or omission, intellectual property theft, trademark or copyright infringement, invasion of privacy, libel or other defamation, and even product disparagement.

The reality of the modern digital age is that challenges to a system can come from distant hackers or those close to a facility's operation. Even if state-of-the-art security controls are in place, there is still a risk from a determined criminal

healthcare report

VICTOR O. SCHINNERER & COMPANY, INC.

Information and Risk Management Ideas for Healthcare Professionals

element that can bring operations to a halt. However, a large proportion of data breaches are not unknown hackers with criminal intent or a desire to cause vandalism to the system, but employees, former employees, or even business partners.

Risks of Data Security Need Integrated Insurance Solutions

Traditional general liability insurance does not address the plethora of cyber exposures that are endemic in the operations of a healthcare facility. As the risks associated with electronic business and communication applications continue to grow, coverage is needed for first-party risks—the losses to the operations of the entity, including intellectual property, data, and sensitive information and network operations. General liability policies exclude most cyber risk damages because the policies are designed to cover physical damage as opposed to damage caused to the operations of an organization. Some carriers have specifically excluded data and technology-related risks from their policies. Property and crime policies may offer only limited coverage, if any coverage is provided. Certainly, the economic losses and exposures related to the professional services performed are excluded from other types of policies.

Security breaches that lead to theft, destruction, or unintended

dissemination of important information damage both the operations of the entity and expose it to third-party risks—the losses sustained by others can include the exposure of bank account information, credit card data, social security numbers, and other private information that can result in identity theft. In addition, an operation could be responsible for virus and spam transmissions that result in damage to the computer systems of others. If an entity's network system is breached, it has a legal duty to inform any clients who could possibly be affected by that breach within a certain period. The time and cost associated with notifying third parties of that breach can be enormous. Credit monitoring and credit repair services also might be required.

Insurance Can Cover the Liability to Others and Damage to the Entity

Integrated insurance coverage combines third-party exposures for cyber liability with first-party coverages for cyber crime-related expenses. The costs related to privacy notification, crisis management, and disaster recovery are often unrecognized. Both direct losses and the legal liability for consequential damages resulting from cyber security breaches are accommodated. Third-party liability insurance provides coverage for harm to others. For instance, insurance solutions can be a major remedy for business interruption (the lost income

from a computer attack or other non-physical peril) as well as for harm to others caused by network or internet security damages. The defense costs and damages arising as a result of breach of confidence or infringement of any right to privacy, intellectual property rights, or statutory duty, such as the notification of those affected by a loss of private information and the provision of credit monitoring, can be mitigated through the proper coverages. And damage to a hospital or healthcare facility's intangible assets such as code and data can be covered.

Risk Mitigation and Insurance Coverage Are Essential

Organizations often fail to realize that exposure to cyber liability affects the bottom line as well as damages relationships with customers, vendors, and partners. Confidential information, content, knowledge, and business intelligence are vital information assets that must be protected.

The establishment of an information security policy, constant vigilance, and the use of sound practices and industry-recognized safeguard processes and technologies create a balance between the technological and procedural aspects of information security management. But the ongoing process of exercising due care and due diligence to protect information and information systems from unauthorized

healthcare report

VICTOR O. SCHINNERER & COMPANY, INC.

Information and Risk Management Ideas for Healthcare Professionals

access, use, disclosure, destruction, modification, or disruption is not the only indispensable part of protecting operations.

Business interruption resulting from a security failure, a cyber extortion threat and the costs related to privacy

notification, the management of an information security failure, and the resulting disaster recovery costs are all challenges to a facility's continued viability. A cyber liability insurance policy is an indispensable part of any healthcare operation's risk management program. With

coverages tailored to meet the unique and evolving cyber insurance needs of hospitals and other healthcare organizations, appropriate insurance and the accompanying risk management services eliminate gaps in insurance coverage and position an entity for continued productivity.

Schinnerer's Cyber Liability Coverage

Schinnerer offers a policy that covers the following:

- **Disclosure Injury:** lawsuits alleging unauthorized access to or dissemination of the plaintiff's private information.
- **Content Injury:** legal actions arising from intellectual property infringement, including patent, trademark, and copyright infringement.
- **Reputational Injury:** allegations of the disparagement of products or services or of libel, slander, defamation, and invasion of privacy.
- **Conduit Injury:** demands for remedies for harm to third-party systems allegedly resulting from system security failures.
- **Impaired-Access Injury:** suits, civil fines, and penalties arising from system security failure resulting in the computer systems of business partners or others being unavailable for use.

Coverage is also needed for first-party cyber-crime expenses—the harm to the hospital or healthcare entity. Schinnerer's options include separate coverages that address:

- **Privacy Notification Expenses:** printing and postage for individual notifications, call center costs and advertisements, cost of credit-monitoring services, credit freezes, and fraud alerts for affected customers.
- **Forensic Costs:** costs to determine how the breach occurred.
- **Crisis Management and Reward Expenses:** including the cost of public relations consultants to maintain the reputation of the business.
- **E-Business Interruption:** including first-dollar extra expense.
- **E-Theft and E-Communication Losses:** extended to networks outside the hospital or healthcare entity's system.
- **E-Threat or Cyber Extortion:** including the cost of a professional negotiator and ransom payment to stop cyber attacks caused by malicious hackers.
- **E-Vandalism Expenses:** paying the costs of malicious damage even when the vandalism is caused by an employee.