Security – What carriers must do

In an interview the Deputy Director of the NSA, Mr. Richard Ledgett, said that "If you are connected to the Internet, you are vulnerable to determined nation-state attackers" citing security incidents such as the Sony hack. He added "As everybody in the world becomes more connected with computers and information systems, the vulnerabilities are going up." This is very true for Insurers as they rollout their digital strategies to provide anytime anywhere access to consumers and agents. Identifying risks, improving defenses and preventing attacks is becoming a key function of corporations.

A classic paper published by SANS institute in 2004 titled "Computer Security and the Law: What you can do to protect yourself" crystallizes what every corporation must do into four core principles:

- Know the System
- Principle of least privilege
- Defense in depth
- Prevention is ideal but detection is a must

While these principles still hold true, the scope and the activities of what corporations must do has broadened and is outlined by NIST Cybersecurity Framework published in 2014. We will summarize the essence of these findings in this paper.

NIST identifies 5 core functions, namely,

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

The tasks that must be fulfilled for each of these functions are categorized into 22 categories and 98 subcategories. We will summarize the tasks to fulfill each function.

Identify requires that a corporation create a detailed inventory of all physical devices, systems and software ("know thy system") and then conduct a risk assessment and identify a risk management strategy. Physical devices will include servers, network components, workstations, laptops, mobile devices, etc.

Systems and software will include all operating systems in use, their versions, all third party software, all applications developed in house, etc. Conducting a risk assessment will require the collection of threat and vulnerability information from vendors (for example Microsoft) and information sharing sources such as CERT.
Protect requires that a very strict access control is in place. Access control for every user and program should only provide the least set of privileges necessary to complete the job. This principle limits the damage that can result from an accident or error. Protect also requires data security. All sensitive data must be encrypted and kept safe. Protective technologies must be used to prevent unauthorized access to data. It also requires compliance with security standards such as PCI DSS for storing and handling financial data.

Statistics show that almost all of the breaches involved stolen credentials. This means that a good security principle for information systems is defense in depth. Defense in depth requires security in each of the layers of the application software, starting with the physical devices (client and host), network, system software, applications, API or web services and the data layer. For example, a firewall can be programmed to block all VPN or HTTP requests from unknown/unusual locations such as from outside the country. And, a data tier can implement row based security and limit data to only those accessible to the current user so that even if one user's credentials are compromised, it does not result in widespread damage. Software, whether developed in house or purchased from a third party, must be tested for common vulnerabilities such as SQL injection, etc.

Another major aspect of the protect function is awareness and training. All users whether internal users, agents or consumers must be made aware of security best practices to prevent accidental errors. Software, where possible, can also influence user behavior by enforcing best practices—for example, strong password policies.

The next step is to monitor for and detect any anomalies. Security requires continuous monitoring. Tools and processes must be put in place to ensure that detection happens. Without them, data breaches can go on for months before they are detected. As noted earlier, prevention is ideal but detection is a must. Keeping an audit trail of who is doing what is critical to identify the problems. Tools are useful in analyzing the large amount of audit logs, identifying unusual patterns and generating alerts or even acting on them intelligently.

Corporations must also plan for eventualities. Good response planning is important to analyze breaches, to communicate correctly to all impacted parties and to quickly address the situation that led to the breach. Recovering from a breach requires identifying improvements and implementing risk mitigation strategies to prevent future occurrences of data breaches.

Security in the modern world is a vast subject. We looked at the core functions and high level tasks to implement a sound security policy. To learn more on these topics, please refer to the excellent resources available online from SANS Institute, NIST and CERT.

If you have a question or comment, please direct your question/comment to vnarayanan@jarushealth.com.

Jarus Health Technologies
681 Anderson Drive
Pittsburgh PA 15220
www.jarushealth.com
Email Id: vnarayanan@jarushealth.com
T: 412-922-5432