Sera-Brynn Sentinel Server™

You can't stop unauthorized access or criminal activity on your systems if you don't know about it.

Every day there are over 2,000,000 attempts to break into the computer and network systems of America's businesses. The Federal government is considering legislation that would mandate reporting any attempted hacking into your commercial systems.

These things can happen to you if you get hacked. They happen every day.

- You will lose money.
- Credit Bureaus can freeze your ability to process credit cards. Your business will shut down.
- You will lose credibility and the trust of your clients and customers.
- You will lose critical intellectual capital. And customer data.
- If their information is stolen from your systems, affected parties (clients, vendors, etc…) may pursue litigation for "willful neglect."
- You may be subject to federal, state and industry specific fines as well as restitution fees.

Examples of HIPAA security fines.

- Cignet Health care of Temple Hills, MD. Fined $4.53m by US Department of Health and Human Services.
- Blue Cross Blue Shield (BCBS) of Tennessee fined $1.5m by US Department of Health and Human Services in addition to the $17m BCBS paid in restitution.
- UCLA Health Systems fined $865,000 by US Department of Health and Human Services.

Most industries require an intrusion detection capability as part of the business's information security strategy. Unfortunately, employing certified Information Security Specialists can be very expensive.

Cybercrime…a growing industry.

- In 2011, foreign cybercriminals hacked into a small bank in Eliot, Maine. They stole $28,000 from one back account alone. The bank never detected the intrusion into their systems and therefore never reacted to stop it.
- Cybercrime is growing... fast. The current annual cost of cyber attacks to businesses is estimated to be $114 Billion. That's more than the illegal global trade of Marijuana, Cocaine and Heroin combined. This is why more and more criminals will be focusing their efforts on Cybercrime in the very near future. No business is immune.

The Sera-Brynn Sentinel Server™ is specifically designed to:

- Let you know of ANY unauthorized attempt to access your computer or network systems, including those from rogue employees.
- Meet commercial industry and Healthcare information security requirements by constantly monitoring the security of your network infrastructure.
- Be easy to interpret…color coded so you can see attempts to break into your systems in seconds. Comes with a mobile app so you can monitor the security posture of your computers and networks from anywhere on the globe.
- Meet all PCI and HIPAA certification requirements. This includes quarterly PCI validation requirements.
- Automatically generate (and send) reports to any designated recipient. This takes care of anticipated mandatory federal reporting requirements.
- Be a cost-effective alternative to the current trend of hiring more security staff.

Sera-Brynn Sentinel Server™

You can't stop unauthorized access or criminal activity on your systems if you don't know about it.

What are PCI and HIPAA?

- The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule is a set of federal regulations regarding the use and disclosure of a person's health records.

Who is Sera-Brynn?

- We are Cyber security specialists with backgrounds in national security and intelligence, international retail, banking, logistics, and finance. Our security professionals maintained the information security systems of the national intelligence agencies. Now we can do the same for you.

Did you know?

- 46 states have now enacted data breach disclosure laws that require businesses to notify customers whose card numbers are stolen. For example, in Virginia the Office of the Attorney General may impose a civil penalty up to $150,000 per breach. And that doesn't include possible fines from banks and credit card companies! American Express recently published fines in excess of $200,000 per month for non-compliance of its vendors.

Do It Yourself

- Hire a Certified Information Security Specialist ($130,000)
- Purchase security management software ($30,000)
- Purchase necessary servers / connectivity hardware ($20,000)

* Note: Figures based off an average network size of 500 computers.

Total $180,000

Sera-Brynn Sentinel Server™

Lease Sera-Brynn Sentinel Server™ ($2,500 / mo)
Includes:

- All Sera-Brynn Sentinel Server hardware and software and set-up ($50,000 market value)
- 24/7 Intrusion Detection for up to 500 clients/machines
- Quarterly PCI Reporting
- Regular Maintenance and Quarterly Site-Visits
- Meet all PCI and HIPAA security requirements
- Sera-Brynn as your Certified third-party Information Security Specialists
- Automatic reporting of intrusion attempts
- Mobile app to monitor security posture from anywhere on the planet

Total $2,500 / month

To learn more about the Sera-Brynn Sentinel Server™, please e-mail us at info@sera-brynn.com, visit our website at: www.sera-brynn.com, or call 757.243.1257.

sera-brynn
information security outfitters