BSSi2

Innovations

Review Twice, Implement Once. Doing IT Right the First Time.

Scott Bernstein, CPA
President

Nick Espinosa
CIO & Chief Security Fanatic

On the Lighter Side

Driving through Southern California, I stopped at a roadside stand that sold fruit, vegetables and crafts. As I went to pay, I noticed the young woman behind the counter was painting a sign. 'Why the new sign?' I asked. 'My boyfriend didn't approve of the old one,' she said. When I glanced at what hung above the counter, I understood. It declared: Local Honey Dates Nuts.

My boyfriend and I met online and we'd been dating for over a year. I introduced Hans to my uncle, who was fascinated by the fact that we met over the Internet. He asked Hans what kind of line he had used to pick me up. Ever the geek, Hans naively replied, 'I just used a regular 56K modem.

About a year had passed since my amicable divorce, and I decided it was time to start dating again. Unsure how to begin, I thought I'd scan the personals column of my local newspaper. I came across three men who seemed like they'd be promising candidates. A couple of days later, I was checking my answering machine and discovered a message from my ex-husband. 'I was over visiting the kids yesterday,' he said. 'While I was there I happened to notice you had circled some ads in the paper. Don't bother calling the guy in the second column. I can tell you right now it won't work out. That guy is me.'

Secure Document Shredding: Best Practices for Disposing of Medical and Financial Records

When you consider the amount of data stored in medical and banking/financial industry offices, you realize the potential for data and identity theft is staggering. It's why a secure document shredding program is of the utmost importance for these types of organizations.

Medical Industry Policies

According to a study in The American Journal of Managed Care, paper and film records are the most common source of data breaches in hospitals. Have you questioned what policies they have in place to ensure that your private paperwork stays secure after it reaches the end of its life?

Doctors' offices and hospitals must walk a fine line between retaining customer records in case they're needed for future reference and protecting patient information. There are specific state laws as well as Health Insurance Portability and Accountability Act (HIPAA) laws that outline the rules around retention of sensitive health documents.

HIPAA, for example, requires that medical records be retained for six years from the date they were created or last used. Individual states have their own laws around medical record retention times, but if those times are shorter than the HIPAA period, the latter will preempt the state law.

Once a medical document has reached the designated time period, it must be securely shredded. The types of records and information covered under HIPAA and state privacy laws include:

- Names
- Social Security Numbers
- Account Numbers
- Medical Record Numbers
- Phone Numbers
- Email Addresses
- Full Face Photos
- Health Plan Beneficiary Numbers
- Vehicle Identifiers and Serial Numbers

Continue on the next page...

Financial Industry Policies

Like the medical industry, the banking/financial industry also has laws that govern how long documents must be kept before they are securely destroyed. These laws include:

- The Equal Credit Opportunity Act, which requires financial institutions to store loan application documents for 25 months after the applicant has been notified of the action being taken
- The Electronic Funds Transfer Act, which requires banks to retain evidence of compliance for two years after the date disclosures are given or any sort of action is taken
- The Bank Secrecy Act, which requires a five-year retention of a variety of documents, from CTRs and SARs to records of cashier's checks of $3,000 or more

It's a good idea to be aware of these laws and which documents are still being held by the financial institutions you've worked with. And, just as with medical offices, have you asked your bank and any financial services companies you work with what their procedures are to ensure that your sensitive information stays secure after it reaches the end of its life?

Insist on Secure Document Shredding

Fast forward. The time has come when your medical and financial service providers no longer need to retain records with your private information. At that stage, all paperwork should be placed in locked paper bins provided by a AAA NAID-certified document solutions company. This will ensure that your documents cannot be tampered with before they are shredded.

If this is how your service providers operate, your paperwork will soon be destroyed — either by a mobile shredding truck that comes to the place of business and destroys the documents on site or in a secure facility where documents are destroyed by professional shredding equipment. What you should also know is that if your medical and financial services providers are using a AAA NAID-certified document solutions company, they can request a certificate of destruction to keep on file to prove that they properly and securely disposed of their clients' or patients' sensitive data.

The next time you have an appointment with a doctor or you visit your bank or financial advisor, ask how they manage your sensitive data – both in the office and when it's time to shred it. If you don't like the answer, feel free to refer them to Paper Tiger for more information about secure document shredding.

Paper Tiger Document Solutions

Paper Tiger Document Solutions offers comprehensive document management solutions for businesses large and small. We can handle all of your document storage and document shredding/ destruction needs - providing you with very competitive pricing, industry-leading service, instant access to, and control of, your data. And, we can provide 100 percent peace of mind.

Web: www.yourpapertiger.com
Location: 1101 N. Estes Street
Gurnee, IL 60031
Phone: 847-599-970
Email: info@yourpapertiger.com

Did You Know? BSSi2 can help you with Employee Phishing Education

Old school Security Awareness Training doesn't hack it anymore. Today, your employees are frequently exposed to sophisticated phishing and ransomware attacks. More than ever, your users are the weak link in your network security. They need to be trained and then stay on their toes, keeping security top of mind.

Baseline Testing
We provide baseline testing to assess the Phish-prone percentage of your users through a simulated phishing, vishing or smishing attack.

Train Your Users
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users
Best-in-class, fully automated simulated phishing, vishing and smishing attacks.

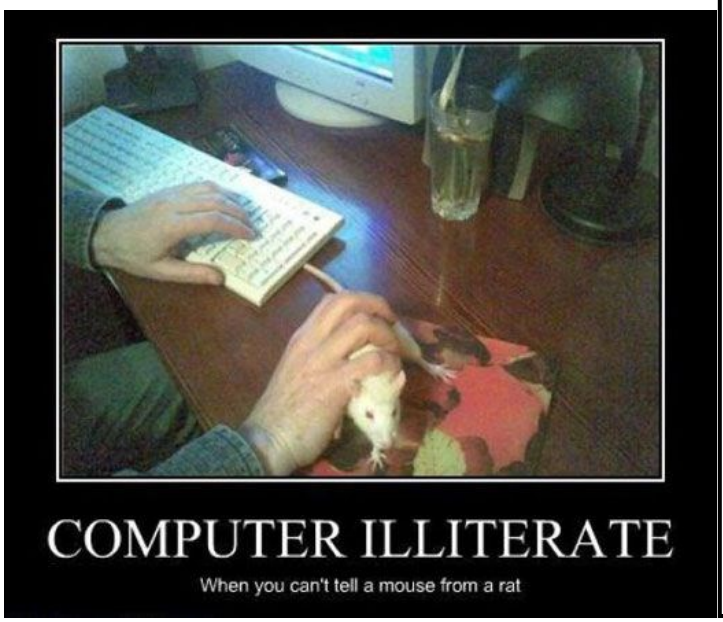
See The Results
Enterprise-strength reporting. Both high-level and granular stats and graphs. We even have a personal timeline for each user.

Just give us a call at 847-551-4626 or email sbernstein@bssi2.com for more information.

Build a More Resilient and Secure Organization

Will Proposed New Laws *Ban* Making Ransomware Payments?

The ransomware scourge has become much worse the last 12 months. Highly organized cybercrime gangs have iterated their attacks into a massive extortion racket.
They are focusing on easy prey, and recently dozens of local governments, school systems and non-profits have been infected, apart from very visible large companies that suffered weeks of downtime.
To avoid disruption, ransomware victims continue to pay up. Well over half decided that downtime would be more expensive than the ransom, including infected local governments.
However, taxpayers don't want their dollars going toward ransomware attacks
A recent survey by PandaSecurity shows that 86% of Americans believe their local government should not pay the ransom on a ransomware attack. Additionally, the results showed that Americans prefer to invest tax dollars in cyber security awareness training and up-to-date software rather than using ethical hackers or insurance.
Enter two senators of New York state. They recently came up with bills to ban government agencies and local municipalities from using public money to pay cybercriminals to get their files back.
The first bill, proposed by Republican NY Senator Phil Boyle, and the second bill, proposed by Democrat NY Senator David Carlucci, are currently in committee.
Several industry experts stated that this is the first time any state authorities have proposed a law that outright bans paying the ransom all together.
We had a brief look at both bills "in committee" (which means that lawmakers discuss to either release or not release the bill to the floor to be voted upon). Neither bill covers cyber insurance which adds another wrinkle to this whole mess.
A law like this could force a restructuring of cyber insurance under NY insurance regulation, and these two bills might never get out of committee because of pressure from the cyber insurance sector.
U.S. insurers are ramping up cyber-insurance rates by as much as 25%
Reuters reported that the price hikes follow a challenging year of criminal hackers using ransomware to take down systems that control everything from hospital billing to manufacturing. "Ransomware is more sophisticated and dangerous than we saw in the past," said Adam Kujawa, director of Malwarebytes Labs.
The average ransom of $41,198 during the 2019 third quarter more than tripled from the first quarter, according to Coveware, which helps negotiate and facilitate the payments.



The Pets of BSSi2

Meet Shannon 's cat:

This is Lucy, she is 15 years young and has been partially blind for most of her life. She doesn't let that stop her from playing with her favorite catnip toys or from navigating the home. She is the softest kitty and anyone who meets her falls in love with her sweetness.

February 2020

35 Aztec Court
South Barrington, IL 60010
(312) 752-4679
www.bssi2.com

"We make all of your computer problems go away without the cost of a full-time I.T. staff"

"I'm just sayin' a little conflict resolution trainin' might not be unwarranted."

Shiny New Gadget of the Month

M&R Digital Counting Coin Bank

Many of us still keep a coin jar to toss our spare change into. Even with the growing popularity of apps like Apple Pay and Google Pay, coins remain a big part of our lives. Of course, when you're tossing coins into a jar at the end of the day, you have no idea how much you've collected until you count it or take it to a Coinstar.

The M&R Digital Counting Coin Bank solves this problem. You never have to count change again. Every time you drop coins into the bank, it counts and adds them to the total. The digital readout keeps you updated on how much you've saved. It's a remarkably simple piece of technology that eliminates the hassle of keeping track of change.

Stay up-to-date with the latest Cybersecurity News!

Follow our Chief Security Fanatic and CIO, Nick Espinosa, on social media for cybersecurity videos and articles:

- www.facebook.com/NickAEsp
- twitter.com/NickAEsp
- www.linkedin.com/in/nickespinosa/

Follow BSSi2 at:

- www.facebook.com/bssi2
- twitter.com/BSSi2llc