FOR MEMBERS ONLY

SMBiSAO

December, 2017
Volume 2

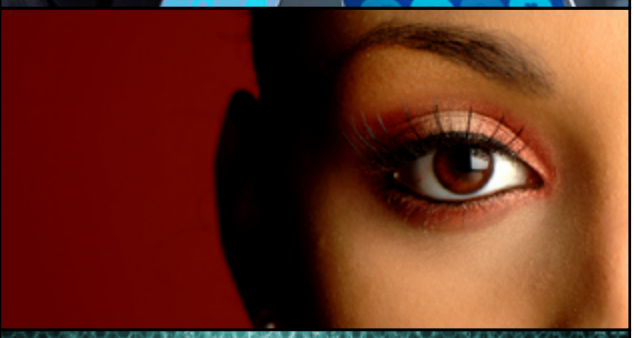
# THE SMB ENTERPRISE

SMB iSAO MONTHLY REPORT



## THE LATEST NEWS





## SMB MUST READS

### Holiday Shipping Scam, a report from Infragaurd

The FBI's Office of Private Sector (OPS) is providing this LIR to private sector partners as awareness that the FBI Internet Crime Complaint Center is warning consumers about a fraudulent email scam. The emails claim to be from one of three shipping businesses and claim that a package intended for the email recipient cannot be delivered. The messages include a link that recipients are encouraged to open in order to get an invoice to pick up the package, however, the link connects to a site containing malware that can infect computers and steal the user's account credentials, log into the accounts to obtain credit card information, additional personal information, and learn about a user's shipping history for future cyberattacks.

The messages may consist of subject lines such as: "Your Order is Ready for Shipment," "We Could Not Deliver Your Package" or "Please Confirm Delivery." The shipping companies say they do not send unsolicited emails to customers requesting information regarding packages, invoices, account numbers, passwords or personal information and if you receive such a notice -- don't respond. You should delete the email immediately or forward it to the companies listed contact email address. If your interaction with the website resulted in financial loss you should contact your bank immediately.

If you unintentionally visited or encountered a site suspected of utilizing this scam, you may also report it to your local FBI Office and/or the Internet Crime Complaint Center (IC3): www.ic3.gov.

## THREAT INTEL REPORTS

### Bitcoin Intensifies Pain for Some as Ransom Demands Skyrocket

By Bloomberg Technology

Hey, want those photos and files back? It may cost more than it used to. Thank bitcoin. Chubb Ltd., best known for catering to wealthy families and corporations, is among at least three insurers facing a jump in costs tied to claims from ransomware attacks. The firms attribute much of that to the surging price of bitcoin, the currency of choice for online extortionists. And that's bad news for everyone. There's been "a massive escalation" in both the number of attempts and the size of demands as criminals scramble for the hot cryptocurrency, said Michael Tanenbaum, an executive vice president at Zurich-based Chubb. "The rise in price of bitcoin correlates," he said in an interview, declining to specify total costs. Around midyear, top payouts in corporate ransomware attacks began to exceed $1 million, dwarfing the previous maximum of about $17,000, he said.

Insurers like Chubb are a good place to look for information on costs from ransomware -- a type of malicious software that blocks access to computer files until victims pay a toll. Globally, security firms say incidents have exploded, ranging from precision hacks to this year's mass assaults, like WannaCry. Insurers have a unique view of what actually gets paid, especially in the most expensive cases, because they may shoulder the burden. Frozen Computers Ransomware incidents have soared in recent years, according to McAfee Inc. Typically, they enlist third-party specialists, such as Kivu Consulting and Navigant Consulting, to facilitate cryptocurrency payments and investigate perpetrators. Those firms say business is booming. This year's frenzy for bitcoin has made hackers bolder, demanding larger payouts, said Winston Krone, a global managing director who oversees Kivu's ransomware services. Demands of $250,000 to $500,000 were nonexistent six months ago, and now they're a weekly occurrence, he said. "We can make immediate payments of six figures," Krone noted. His firm has teams of multi-lingual investigators trained to negotiate with hackers or ensure clients aren't dealing with a terrorist group, which can run afoul of U.S. laws. Short of that, it's the customer's decision whether to give in to extortion, he said. "The ethics of paying ransoms and paying criminals, we take a neutral stance."

#### Trending IOCs

(Indicators of Compromise)

- Towercommunitybankmortgage.org
- Summitbank.org
- Newdomains.csv
- Destdir/$today.txt
- /tmp/wget_xxxxxx.zip

#### Trending Malware

- Trending Malware
- RIG
- HANCITOR
- WEBSHELL
- TESLACRYPT
- MIMIKATZ

It might seem counterintuitive that ransoms would rise because of bitcoin's price. After all, the cryptocurrency can be split into tiny fractions, allowing payments of any amount. But some extortionists have been slow to adjust bitcoin-denominated demands amid the rally, according to Christiaan Beek, who leads strategic threat intelligence research for McAfee Inc., the cybersecurity firm. A criminal network initially seeking a few bitcoins per victim might keep collecting that amount for months. Yet this year the digital currency has climbed ever upward, from roughly $1,000 in January to surpass $19,000 this week. "Because the price of bitcoin has seen a dramatic spike in the latter half of 2017, it has made the overall price of demands much larger," said Kimberly Horn, an executive at insurer Beazley Plc who oversees breach-response and information-security claims.

Ransomware claims at Beazley are on pace to rise more than 70 percent this year to 260. McAfee projects average payouts are about $900 to $1,200, up from roughly $600 in 2015. XL Group Ltd., another insurer, said it's fielding demands of $20,000 to $60,000 -- compared with about $300 before bitcoin took off. To be sure, observations vary. Symantec Corp. said it sees more instances of hackers ratcheting up the frequency of their attacks, while tempering individual demands to ensure victims will pay. In contrast to McAfee, Symantec estimates average ransom demands may even drop this year. There are additional trendsdriving up total costs. Early ransomware attacks proved people and companies are willing to pay, luring more opportunists. Pioneering hackers are now flanked by rogue nations and novices. Extortionists can buy malicious software on the dark web and pump out emails to infect computers. There were more than 12 million attacks in the third quarter of this year, up from roughly 4 million in the same period of 2015, according to McAfee. And many people don't have policies to offset their costs.

**>> READ MORE**

THE SMB ENTERPRISE

December, 2017 Volume 2

## MEMBER FORUM AND INFORMATION SHARING

### MEMBER FORUM

**Cyber Risks – The Tip of the Iceberg**

2017 may be known as the year the U.S. SMB world really got a glimpse of the cyber-crime iceberg that lurks underneath the water line. In June, the world's largest container ship operator, A.P. Moller-Maersk, fell victim to the global Petya cyberattack. The malware originated in Ukraine, but spread like wildfire through Maersk's global IT systems. Several port terminals run by a Maersk division, including in the United States, India, Spain, the Netherlands, shut down for days and cost the company up to $300m. In the wake of the Maersk attack, my office fielded panicked calls from small and medium sized coffee importers who had been alerted that their containers of specialty coffee were essentially "lost at sea." In this case both the coffee and the ship were 'found' and no claim filed…but it could have been worse. How would these business owners have continued with their supply chain totally disabled?

Indeed, cyber pirates can be more than thieves. Earlier this year, a small batch coffee roaster in the…

>> READ MORE

### LEGAL CORNER

Cybersecurity is a relatively new and evolving field of technology, law, and regulation. The uncertainty and evolutionary state of the industry pose unique challenges to business leaders. In addition to deploying effective technical security strategies, companies need to be prepared to mitigate the direct damages from criminal, civil, and regulatory liabilities that can flow from a cyber security event. Today 47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted their own laws pertaining to an organization's requirement to notify their customers and other parties about the breach and take other steps to remediate injuries caused by the incident. Each of these State laws define differently a company's obligations, what constitutes personal information, notice methods, and exemptions.

It is unrealistic to expect an SMB business to know all the myriad of data privacy and data breach laws. However, business leaders need to know who to call if they believe a breach has occurred. Experts such as information sharing communities like the SMB iSAO, cybersecurity lawyers, and cyber insurance providers can help sort through the…

>> READ MORE

### WHAT'S NEW FOR ISAOs? THE SO UPDATE

**ISAO Standards Organization Proposes Voluntary Certification Program Addressing Future Needs of the ISAO Ecosystem**

The ISAO SO announced at the recent International Information Sharing Conference (IISC) held in Washington D.C. October 31 – November 1 the intent to move forward on a potential certification program. The purpose of the program, as outlined in a presentation by Dr. Gregory White, the Executive Director of the ISAO SO, is to address the future needs of the ISAO ecosystem in terms of several factors:

How does a prospective member of an ISAO know which ISAO they may want to be a member of? How does the prospective member know what services and capabilities are important and whether a specific ISAO can provide those services and capabilities?

How is trust established in a TIMELY MANNER between ISAOs or between an ISAO and the government? How is this accomplished when the ecosystem consists of hundreds or thousands of ISAOs? How is this accomplished across international borders?

Currently there is no control regarding who can call their organization an ISAO or an ISAC. A prospective member considering joining an ISAO would not have any way to know what that means in a given situation. If the ISAO was self-certified the prospective member would know that the organization at least claims to provide certain services and capabilities and there would be some consistency between ISAOs. If the ISAO was third-party certified then the prospective member would know even more and would have some level of confidence because of the certification that the ISAO is providing the stated services and capabilities.

Dr. White stated that the ISAO SO proposes to develop initial thoughts on a voluntary certification program that could address the above issues and to publish it in November for comments from the public. At the same time, the ISAO so…

>> READ MORE

***Have a story you'd like to share anonymously?***

**Send it to info@smbisao.com**

## THE LAST WORD

### TIP OF THE MONTH

**This month's Tip of the Month section is brought to you by the Small Business Association.**

1. **Protect against viruses, spyware, and other malicious code:** Make sure each of your business's computers are equipped with antivirus software and antispyware and update regularly. Such software is readily available online from a variety of vendors. All software vendors regularly provide patches and updates to their products to correct security problems and improve functionality. Configure all software to install updates automatically.
2. **Secure your networks:** Safeguard your Internet connection by using a firewall and encrypting information. If you have a Wi-Fi network, make sure it is secure and hidden. To hide

>> READ MORE

### RECOMMENDED READING

**This month's recommended reading is from Biz Journals, titled, "The three B's of cybersecurity for small business."**

Large-scale cyberattacks with eye-watering statistics, like the breach of a billion Yahoo accounts in 2016, grab most of the headlines. But what often gets lost in the noise is how often small and medium-sized organizations find themselves under attack. In the last year, half of American small businesses have been breached by hackers. That includes Meridian Health in Muncie, Indiana, where 1,200 workers' W-2 forms were stolen when an employee was duped by an email purporting to come from a top company executive. Many small companies are just one fraudulent wire transfer away from going out of business. There's lots of advice available about how to fight…

>> READ MORE

**Want to sponsor our next issue of the SMB Enterprise? Space available. Please send request to info@smbisao.com**

Sponsorship request

### NOTES FROM OUR SPONSOR

HIPAAgps is excited to be this month's sponsor of SMB iSAO's The Enterprise. We believe the ability to share cybersecurity threats and information on how to protect against them is a valuable resource. This is especially true for organizations that work within the HIPAA compliance realm. There are many small to mid-sized health care entities and business associates that can benefit from this information sharing. The threat of unauthorized disclosure of PII has increased substantially as more bad actors are using ransomware and malware to gain access to protected health information (PHI). Using lessons learned from previous HIPAA breaches can help reduce the cost of protecting networks and PHI from prying eyes.
**Please visit www.hipaagps.com for more information.**

HIPAAgps

### THIS MONTH'S SURVEY

**Question:**
What are your biggest cybersecurity fears or challenges as a small business owner? What would help to overcome these obstacles?

**Your thoughts:**

Submit your survey answer

## CONTINUED ARTICLES

### Bitcoin Intensifies Pain for Some as Ransom Demands Skyrocket *(Continued from page 2)*

Ransom insurance started as a niche in the 1970s, pioneered by firms including Lloyd's of London Ltd. and American International Group Inc. Companies concerned about executive abductions and wealthy families vulnerable to kidnappings snapped up coverage. Over the years, some policies added protection for online extortion. Insurers also rolled out separate products for cyber-attacks. Ransomware is now rattling that market. In May, days after WannaCry grabbed global headlines, law firm Covington & Burling posted a memo to clients, warning them to review terms in their contracts. Within general kidnapping policies, there often was little to no deductible for online extortion schemes, said Anthony Dagostino, global head of cyber risk at Willis Towers Watson. But that's changing. "The insurance companies woke up to this, saying this is almost way too much," said Dagostino, whose firm doesn't provide cyber coverage but works with clients to find a carrier. "We're already getting word that some insurance companies are not providing the coverage or are adding to the deductibles."

***Care to respond to this story? Join the forum! Visit your member portal at www.smbisao.com and post your thoughts.***

### LEGAL CORNER *(Continued from page 3)*

confusing regulatory requirements. You also need to familiarize yourself with the various data protection standards for specific industries and specific business practices. For example, the PCI credit card security standards and the federal data security regulations regarding HIPAA information are specific as to how your organization needs to handle these protected data sources.

Today the state of cybersecurity law is unfortunately piecemeal. Statutes, regulations, and common law standards describing a corporation's cybersecurity obligations are scattered across state and federal law. This fragmentation is a challenge for businesses in understanding what their legal obligations are. This complicated landscape creates numerous challenges for decision-makers of companies and requires that corporate leaders educate and prepare themselves both to defend against a potential breach and how to coordinate the response that comes after.

*About The Osinoff Group: The Osinoff Group helps safeguard your sensitive data from insider and outsider threats. We combine deep experience with world-class security solutions designed to secure your business from cybersecurity breaches. The Osinoff Group deploys a data-driven, evidence-based data security model that provides true visibility into current security preparedness, the devices that are connected to the network and actionable insights into vulnerabilities, priorities and remediation.*

### ISAO Standards Organization Proposes Voluntary Certification Program Addressing Future Needs of the ISAO Ecosystem *(Continued from page 2)*

Ransom insurance started as a niche in the 1970s, pioneered by firms including Lloyd's of London Ltd. and American International Group Inc. Companies concerned about executive abductions and wealthy families vulnerable to kidnappings snapped up coverage. Over the years, some policies added protection for online extortion. Insurers also rolled out separate products for cyber-attacks. Ransomware is now rattling that market. In May, days after WannaCry grabbed global headlines, law firm Covington & Burling posted a memo to clients, warning them to review terms in their contracts. Within general kidnapping policies, there often was little to no deductible for online extortion schemes, said Anthony Dagostino, global head of cyber risk at Willis Towers Watson. But that's changing. "The insurance companies woke up to this, saying this is almost way too much," said Dagostino, whose firm doesn't provide cyber coverage but works with clients to find a carrier. "We're already getting word that some insurance companies are not providing the coverage or are adding to the deductibles."

***Have a story you'd like to share anonymously?***

**Send it to info@smbisao.com**

CONTINUED ARTICLES

## CYBER RISKS – THE TIP OF THE ICEBERG *(Continued from page 3)*

Pacific Northwest contacted me wondering if they had an insurance claim. Their IT system had not only been shut down by a ransomware attack, but these mean-spirited hackers had also taken control of the coffee roaster. The cyber criminals demanded an extortion payment, and when payment wasn't received they remotely turned to the roaster to full heat. The owner could not control the machine. Not only did this specialty roaster lose and entire batch of coffee, but the roasting machine almost caught fire, causing serious damage to the machinery and threatening the entire business operation.

Several news agencies have noted that in 2017 the number of things connected to the internet has now exceeded the number of people on earth! And given that in 2017 we have seen cyber-attacks on the largest companies in the world, such as Maersk, and the smallest, such as my roaster friend, it's clear that all businesses are susceptible to cybercrime. In fact, many times SMB's are targeted by cyber criminals because they have fewer resources to put toward IT personal and they generally fail to make cyber security a part of company culture. Likewise, there is evidence that in the event of a cyber incident, SMB's suffer a disproportionate impact compared to larger companies.

Businesses which are victim to cyber-attacks may experience financial penalties, legal costs, loss of consumer confidence, and damage to their reputation. The new reality is that cyber events easily cascade across international borders and industries and may effortlessly disrupt every part of your business. That's why the best businesses understand that cybersecurity is both an operational threat and a long term strategic business risk.

### Some Safety Steps

SMB's should prepare a contingency plan in the event of a cyber breach of not only their system, but also every counterparty in the supply chain or business sphere. The most important asset of an SMB is their people – and it's no different for cyber security. Make cyber training and good cyber practices a priority. There should be a plan for data security which is evaluated yearly. Finally – the board or SMB owner should be involved in cyber security decisions.

### Insurers Respond

The conventional insurance market is scrambling to match wits to cyber criminals and adjust limits to cyber exposures by endorsing commercial policies. However, these insurance "freebies" are typically inadequate to the unique exposures of the SMB. For better protection, many companies choose to purchase a stand-alone cyber insurance policy with coverage tailored to their specific needs. Besides offering stand-alone limits for cyber related losses, insurance companies bring value by helping businesses put in place a strategic approach to cybersecurity. This means strong risk mitigation processes and lightning fast breach responses solutions. A good cyber insurance policy will not only indemnify your covered losses, but also provide for experts to handle your breach crisis.

"Most cyber insurance policies focus on data breach, but the truth is that cyber also touches literally the whole spectrum of risk - it can cause explosions, bodily injury, product recall and so on," says Joshua Motta, CEO at Coalition, a new cyber risk solution offering both insurance coverage and cybersecurity products for the tea and coffee industry. "A good cyber insurance policy should provide risk management and strategic solutions. Otherwise, it's like eating soup with a fork." SMB's need to be keenly aware of their cyber and supply chain risks as well as the limits of cyber, property, general liability when buying insurance. Ask your broker how cyber insurance would respond to business interruption, damage to property, and 3rd party liability claims. If it all sounds confusing…that might be because it is. Fortunately, your SMB iSAO membership carries with it access to a pre-vetted insurance policy with member negotiated rated. Don't wait until you hit the cybercrime iceberg underneath the water!

*Adam C. Rekerdres, MBA, CIC, ACI, is Vice President at Rekerdres & Sons Insurance Agency Inc. and can be reached at adam@reksons.com*

## CONTINUED ARTICLES

### TIP OF THE MONTH *(Continued from page 4)*

your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password protect access to the router.

3. **Establish security practices and policies to protect sensitive information:** Establish policies on how employees should handle and protect personally identifiable information and other sensitive data. Clearly outline the consequences of violating your business's cybersecurity policies.

4. **Educate employees about cyberthreats and hold them accountable:** Educate your employees about online threats and how to protect your business's data, including safe use of social networking sites. Depending on the nature of your business, employees might be introducing competitors to sensitive details about your firm's internal business. Employees should be informed about how to post online in a way that does not reveal any trade secrets to the public or competing businesses. Hold employees accountable to the business's Internet security policies and procedures.

5. **Require employees to use strong passwords and to change them often:** Consider implementing multifactor authentication that requires additional information beyond a password to gain entry. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multifactor authentication for your account.

6. **Employ best practices on payment cards:** Work with your banks or card processors to ensure the most trusted and validated tools and anti-fraud services are being used. You may also have additional security obligations related to agreements with your bank or processor. Isolate payment systems from other, less secure programs and do not use the same computer to process payments and surf the Internet.

7. **Make backup copies of important business data and information:** Regularly backup the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files. Backup data automatically if possible, or at least weekly, and store the copies either offsite or on the cloud.

8. **Control physical access to computers and network components:** Prevent access or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft or can be lost, so lock them up when unattended. Make sure a separate user account is created for each employee and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel.

9. **Create a mobile device action plan:** Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access the corporate network.. Require users to password protect their devices, encrypt their data, and install security apps to prevent criminals from stealing information while the phone is on public networks. Be sure to set reporting procedures for lost or stolen equipment.

10. **Protect all pages on your public-facing websites, not just the checkout and sign-up pages.**

## CONTINUED ARTICLES

### RECOMMENDED READING *(Continued from page 4)*

cybercrime, but it's hard to tell what's best. I am a scholar of how businesses can more effectively mitigate cyber risk, and my advice is to know the three "B's" of cybersecurity: Be aware, be organized and be proactive. Here's how more companies can boost their cybersecurity preparedness without breaking the bank.

Be aware Almost any company can be vulnerable to a range of cyberattacks. A company manager or network security professional needs to know about the various types of digital threats and how to limit vulnerability. There are some attacks that every employee should know about. The most common attacks use a method called "phishing," or a variant that specifically targets one potential victim, called " spearphishing." These typically take the form of email messages that appear to be sent by coworkers or supervisors asking for sensitive information. That's what happened to the health care company in Muncie. These messages can contain instructions that a victim might follow, believing them legitimate – such as clicking a link that installs malware or captures login information, or even making a wire transfer to another business's account. The best defenses against these types of attacks involve skepticism and vigilance. Attackers can be very clever and persistent: If just one person has one weak moment and clicks on one malicious link, an entire network can be compromised.

Be organized Most companies go to great lengths to protect their physical assets and personnel. But many do not take similar precautions with their digital information. A key computer may be kept disconnected from the internet, but if it accepts flash drives or rewriteable CDs, or if its password is easy to guess, the information is just as vulnerable. Small business owners need to prioritize cybersecurity. Without proper preparation, even large companies can find themselves unprepared for cyberattacks. When Sony was hacked in 2011, it did not have an executive focused solely on information security. But hiring someone did not prevent another hack in 2014.

Be proactive Planning ahead is vital, instead of just being reactive. The National Institute for Standards and Technology Cybersecurity Framework lists five main functions of cybersecurity efforts: Identify vulnerabilities, protect against attacks, detect anyone who gets through, respond to the attack quickly and recover after the attack has been stopped. Some companies are already receiving advice that following the NIST guidelines can reduce legal liability if cybersecurity problems arise or are discovered. Companies can also work with colleges and universities to create cybersecurity clinics, or even consider buying cyber risk insurance. There's no way to avoid being the target of a cyberattack, but that doesn't mean becoming a victim. Simple steps can have huge results: The Australian government reported resisting 85 percent of cyberattacks by taking three basic steps: restricting which programs can run on government computers, keeping software updated regularly and minimizing the number of people who have administrative control over networks and key machines. Cybersecurity doesn't have to be rocket science; it's just computer science.