COMMUNITY INSTITUTION & ASSOCIATIONS RISK SUMMARY REPORT

Week of March 12

TLP: Green | ACTL: Guarded | PTL: Guarded | Terrorism TL: Elevated | Follow Us

STOP | THINK | CONNECT™

In This Issue

News and Risk Information

Summary:

Below are some of the top news and risks that the Financial Services Information Sharing Analysis Center (FS-ISAC) has observed this week for community institutions (CI).

NEWS

Experts: It's Time for The US to Get Serious About Cybersecurity. The War Games: From Battlefield to Ballot Box panel comprised of Jason Chen (Mach37), Ann Cox (DHS), Robert Johnson (Adlumin) and Jennifer O'Daniel (Center for Innovative Technology) warned the US is extremely vulnerable to cyberattacks from nation-states and private hackers, and it's time for the nation to get serious about cybersecurity. The country's infrastructure, hospitals, electric grid and organizations of all sizes could be targeted over the next several years, the experts warned. (Fast Company)

Cyber Insurance: Analysis of Problems Related to IT Risk Insurance. Insurance policies have emerged on the insurance market for cyber-risk assurances, which make it possible to transfer at least part of the risk associated with potential cyber-attacks. However, today's insurance companies - unlike, for example, auto or life insurance -- do not have a great deal of data to create models to calculate risk in the cyber-realm. Therefore, more comprehensive and reliable cyber-intelligence data is needed to increase the risk appetite of insurers. (Forbes).

Yahoo Will Face Lawsuits from Data Breach Victims, Judge Orders. Verizon's attempt to have a US District Court dismiss claims against Yahoo for data breaches that affected three billion users has largely failed. US District Judge Lucy Koh has ruled that victims of the breach can now pursue lawsuits against the company for the three breaches that occurred between 2013 and 2016. (Reuters)

RISKS

Industry and Regulatory Roundup: Fraud. The US Secret Service recommends that institutions contact their ATM service providers for the latest security updates and patches to mitigate the risk from ATM Jackpotting, to ensure proper physical security controls limiting access to the machine and to monitor for communications failures and alarms. The jackpot schemes involve thieves posing as ATM technicians, replace the original hard disk with a disk that mirrors the ATM's own software, so fraudsters can remotely control the ATM and force it to spit out cash like winning slot machines. FS-ISAC has also issued information on the attacks. (FICO)

Qwerty Ransomware Utilizes GnuPG To Encrypt A Victims Files. A new ransomware has been discovered that utilizes the legitimate GnuPG, or GPG, encryption program to encrypt a victim's files. Currently in the wild, this ransomware is called Qwerty Ransomware and will encrypt a victim's files, overwrite the originals and then append the ". qwerty" extension to an encrypted file's name. It appears likely that it is manually installed by the attacker when they hack into computer running Remote Desktop Services. (Bleeping Computer)

This Week's Top Risks

- **Malware, Ransomware and Trojans**
  - Cisco
  - Cryptominer
  - Emotet
  - Retefe
- **Physical Security**
  - NY helicopter crash
  - Package Bombing in Austin, TX
- **System Vulnerabilities (multiple)**
  - Adobe, AMD, Apache, EMC, IBM, Joomla, Microsoft, Red Hat
- **Themed Phishing Campaigns**
  - Bank-themed (multiple)
  - Bank Remittance - SWIFT
  - Closing Document
  - Loan #: 0103275632
  - Outstanding payment/ORDER NO.:108
  - Spectra Audio Visual

The Financial Services Information Sharing and Analysis Center (FS-ISAC) is a non-profit corporation that was established in 1999. FS-ISAC is a member-driven organization whose mission is to help assure the resilience and continuity of the global financial services infrastructure and individual firms against acts that could significantly impact the sector's ability to provide services critical to the orderly function of the global economy. FS-ISAC shares threat and vulnerability information, conducts coordinated contingency planning exercises, manages rapid response communications for both cyber and physical events, conducts education and training programs and fosters collaborations with and among other key sectors and government agencies.

This Week's Threat: Incident Response

Malware, phishing, system vulnerabilities: Does your institution have an adequate incident response plan?

Summary:

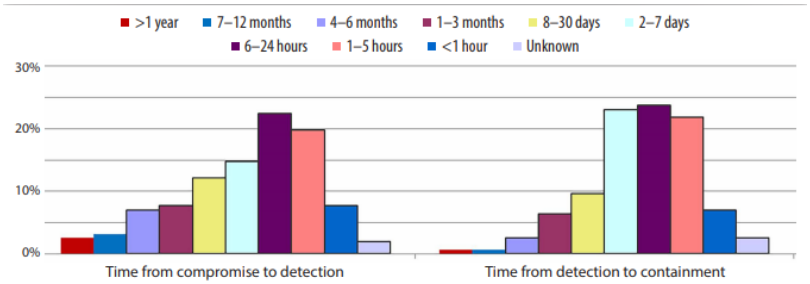
This week, FS-ISAC members have reported numerous security attacks involving credential harvesting malware, phishing and redirect websites. If successful, this type of attack can potentially compromise your or your customer/members network which pulls several adverse triggers. An incident response plan ("IR") should outline *how* an organization is going to respond to an incident. The plan must be tested to determine its completeness and effectives to limit the damage that can impede operations and financial, legal, reputational and regulatory impact.

The following information was obtained in the 2017 SANS Incident Response Survey. It looks at the breakout of organizational size, to better discern whether IR is largely a problem for small, medium or large organizations. The strong representation of both small and midsize organizations solidifies the message that all IR teams are hearing: Attackers are not picky, and everyone is a target. The report states, "Modern threats are no longer limited to massive organizations with significant intellectual property or financial transactions. As commodity threats such as ransomware continue to rise, organizations of all sizes are finding that IR teams, no matter how small or large, are a critical part of the business."

In both 2016 and 2017, 87% of our respondents reported responding to at least one incident within the past 12 months. Of these groups, 21% in 2016 and 20% in 2017 reported responding to at least 100 incidents. When compared against organization size, the survey results indicate that, as expected, larger organizations respond to more incidents than smaller organizations.

In previous years, the IR survey has looked at two key time frames: time from compromise to detection (the "dwell time") and the time from detection to remediation. Containment is a crucial step in the IR process and is the goal that IR teams work toward before achieving remediation. In some cases, remediation and containment are performed in unison, but often they are separate goals.

This year, 50% of respondents reported a dwell time of fewer than 24 hours, a sizable increase from last year's results, in which 40% attained that measure! Additionally, 53% reported a detection to containment time of less than 24 hours in 2017. More than ever, these are obvious signs that our IR teams and times are improving. The figure to the right (*courtesy of SANS*) provides a breakdown of both dwell times (compromise to detection) and detection to containment times.



Approximately 82% of this year's survey base reported that remediation activities take place within one month of containment, with 33% performing these activities within 24 hours. Attackers often only need one incident to convert to a breach, and they can do so very quickly. IR teams should interpret these results as confirming that their investments in detecting incidents are paying off by preventing breaches and that their organizations may be experiencing increased security. Additionally, such results can also help the information security department evaluate whether investments in certain areas are yielding a greater return on investment than others and assist in future budget prioritization.

This year's survey indicated that although IR teams are seeing improvements, root causes of incidents remain consistent. Malware infections were the root cause of incidents or confirmed breaches for 68% of respondents closely followed by unauthorized access, data breach, advanced persistent threats and insider breaches.

The report concludes saying 2016 fostered growth for IR Teams; budgets continue to improve, providing opportunities to hire additional staff and/or train existing team members.

Risks to Organizations:

- Many organizations are on the right track by having an IR plan**;** we receive many requests from institutions for material related to establishing a program. It is crucial that these IR programs are regularly tested to validate their strength, identify gaps and develop controls to fill gaps.

Remediation:

- FS-ISAC's Cyber-Attack Against Payment Systems (CAPS) exercise is an excellent way to test your plan process. The exercise is available to all financial institutions. It is a confidential two-day, tabletop exercise that simulates an attack on payment systems and processes. During the exercise**,** participants begin to draw conclusions and review their internal process**,** and this serves to validate procedures in place, identify opportunities and incorporate additional control objectives or operational processes. For more information, please visit: fsisac.com/Exercises-CAPS.

Understanding the Traffic Light Protocol

Our four-part series explaining the purpose of FS-ISAC's TLP and how it applies to each member

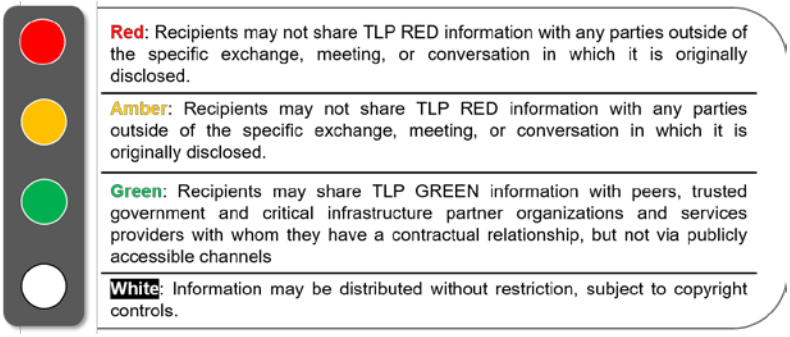
An Introduction

Some time ago, FS-ISAC adopted a Traffic Light Protocol often referred to as "TLP." This TLP is a strict policy that protects safe harbor reporting, confidentiality and privacy of members sharing information in an attributed or non-attributed manner. A large part of "strength in sharing" is the confidence a member has that this information remains within the FS-ISAC community and is shared nowhere else. All information submitted, processed, stored, archived or disposed of is classified and handled in accordance with the TLP classification.

Upon joining FS-ISAC, members agree online or through a signed agreement to follow the FS-ISAC Operating Rules. The Operating Rules obligate all users to abide by the TLP and it is used by originators of shared information to classify that information and to inform recipients how it is to be handled and disclosed to other parties. For more information about the TLP, please refer to the Section 5.1 of this guide and consult the Operating Rules.

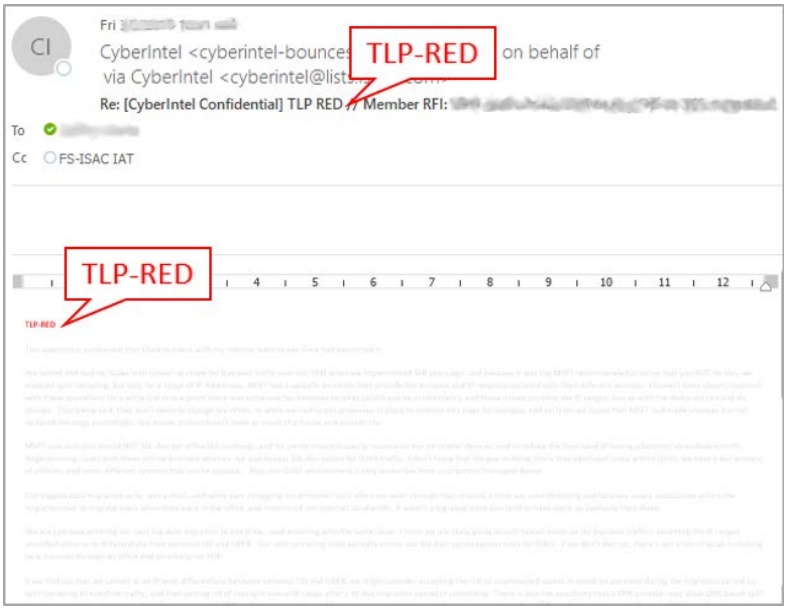
Members can add TLP classifications to subject lines, at the beginning of their content or through the Portal Member Submission tab.

Unless otherwise specified, all information is treated as confidential information (TLP Amber) and is not disclosed to parties outside of FS-ISAC without the permission of the originator. Over the next four weeks we will examine the TLP and provide examples of the types of information.



TLP Red

This real example is a member post to the Cyber-Intel mail list. Taking a moment to review it, you will note in the subject line and body of the email this member has indicated that the contents of this post is **TLP RED**.



That means recipients may not share this information with *any parties outside of the specific exchange, meeting, or conversation* in which it is originally disclosed; the information's audience must be tightly controlled, *because misuse of the information could lead to impacts on a party's privacy, reputation or operations*.

Members violating the TLP risk their institution's continued membership with FS-ISAC. That's right, your membership can be revoked if you violate the TLP pending the results of FS-ISAC's investigation.

If you are the point-of-contact for your institution and you have additional staff receiving information from FS-ISAC, it important all institution staff understand their role in protecting the confidentiality and privacy of all FS-ISAC members.

In Conclusion

FS-ISAC wants its members to share information; however, because information has so much value attached to it, we must do so in a safe and reasonable manner – it is for everyone's best interests.

While TLP Red alerts and communications are infrequent, it is *each member's responsibility* to use the TLP process in accordance with their signed member and non-disclosure agreements. We are only as strong as our weakest link.

Next week we shall look at the most common classification: TLP Amber.

Vendor Oversight: Risk Assessment

Vendor oversight is amongst community bank and credit union regulator focus

Summary:

In part four, we discuss the importance of the risk assessment process. Last week we learned how risk management is the process of identifying, measuring, monitoring, and managing risk and that risk exists whether your institution maintains information and technology services internally or elects to outsource them.

Outsourced services can increase the level of risk for an institution. To reduce the level of exposure risk assessments:

- Assess the risk from outsourcing;
- Involve stakeholders in creating risk-based written requirements to control an outsourcing action; and
- Use the written requirements to guide and manage the remainder of the outsourcing process.

What Risk?

Operational risk may arise from fraud, error or the inability to deliver products or services, maintain a competitive position or manage information.

Operational risk not only includes operations and transaction processing, but also areas such as customer service, systems development and support, internal control processes and capacity and contingency planning.

Strategic	• Planning, implementation, scalability
Compliance	• Legal and regulatory requirements
Reputational	• Errors, delays, omissions, fraud, breaches
Interest Rate	• Errors, inaccurate assumptions
Liquidity	• Service disruptions, settlement delays
Cyber	• Disruption, malware

Service Provider Selection

After identifying the work to be performed and the necessary controls, a financial institution solicits responses from prospective service providers.

Due Diligence

Due diligence should serve as a verification and analysis tool, providing assurance that the service provider meets your institution's need. You should also consider their overall corporate history, financial condition, service delivery capability, internal controls, history of managing sub-contractors, legal and regulatory compliance, adequate insurance, disaster recovery/business continuity (BCP) and visiting the vendor's site.

Quantify Your Risks		
Outsourced Activity Criticality Data sensitivity Transaction volume	Service Provider Financial strength Industry experience Location	Technology Reliability Security Scalability

Contract Issues

The contract is the legally binding document that defines all aspects of the servicing relationship. A written contract should be present in all servicing relationships. This includes instances where the service provider is affiliated with the institution.

Common provisions in the contact would include: Scope of service; security and confidentiality; audits; reporting, BCP; subcontracting; regulatory compliance; performance standards. Remember to notify your regulator (Bank Service Company Act) within thirty days into the contract, performance of services or whichever occurs first.

Next week we will focus on our final article, ongoing monitoring of your vendors.

Questions:

If you have any questions about this week's report, please contact Community Institution & Associations. Content provided for internal use by FS-ISAC members. Copyright owners retain all copyrights to material referenced.

Member Services:
admin@fsisac.com
Toll-Free: 877-612-2622 – prompt 1 Outside US: 1 571-252-8517

FS-ISAC Analysis Team:
IAT@fsisac.com
Toll-Free: 877-612-2622 – prompt 2

For more TLP White about FS-ISAC information, follow us on Twitter @FSISAC and join the discussion on LinkedIn.