Contact Us

Search

securitycurrent

- News
-
- Research
-
- Analysis
-
- Industry
-
- CISO Journal
-
- Podcasts
-
- Company Listings
-
- Webinars
-
- Contributors
  - Key Contributors
  - Guest Contributors
  - Aimee Rhodes
  - Bob Tarzey
  - Charles Kolodgy
  - Christine Vanderpool
  - David Cass
  - David Hahn
  - David Sheidlower
  - David Sherry
  - Fahmida Y. Rashid
  - Farhaad Nero
  - Gary Hayslip
  - Joel Rosenblatt
  - John J. Masserini
  - John Pescatore
  - Larry Whiteside Jr.
  - Linda Musthaler
  - Mark Rasch
  - Mike Saurbaugh
  - Paul Robertson
  - Randy Marchany
  - Richard Stiennon
  - Steve Hunt
  - Victor Wheatman
  -
-
- Newsletter
-
- Library
  - Executive Overviews
  - White Papers

- eBooks
-
-

Home ► CISO Journal ► 'Tis the Season for Cybercriminals - Part One

GSIS

'Tis the Season for Cybercriminals - Part One

December 2, 2015

By Anthony Scarola
TowneBank CISO

In this two-part series, CISO Anthony Scarola examines the elevated threats for both shoppers and financial institutions during the holiday season and offers best practices for ensuring your enterprise is protected during the time of increased risk.

Ho, Ho, Ho! Happy Holidays to the security executive protecting banks across the US! Are you ready for the time of joy and giving? Are you ready to handle the increased cyberattacks and fraud?

'Tis the season for celebrating, spending quality time with family and friends, enjoying delicious home-cooked meals, and for giving unconditionally. Hundreds of billions of dollars will be spent this year to purchase gifts in stores and online, and sadly, many Internet purchases will be performed from hacked computers.

If they are not already pwned, many will be after their employees open social engineering (aka phishing) emails and click on links or attachments containing malware. This will allow criminals to access computers remotely, steal sensitive data capture keystrokes or even access the webcam. Or, more commonly, to encrypt valuable documents and pictures for a hefty ransom.

So, you can say 'tis also the season for criminals to receive! Bah humbug is right! How can you prepare to address the increased fraud and cybercrime against your computer systems and your customers' this season? My friend Dennis Teague, CISO for MainSource Bank, said it best: "You must apply security control 'layers' like onions and ogres." Applied appropriately, individual security control layers will work together to better protect your entire computing environment.

Ransomware malware allows cyber criminals to encrypt data on computer hard drives and shared network folders, locking it with a 'key,' and prompting you to pay a ransom. The ransom is typically requested in Bitcoin due to its anonymity and un-traceability. After a ransomware attack, some customers may call you, their banker, asking for your help and guidance.

Law enforcement and the FBI generally suggest paying the ransom as the cybercriminals usually will send you the decryption key after, but not always. Recommendations for customers to combat this threat, besides the standard message of not clicking on links or opening attachments in unsolicited emails, are to have good response plans including backups of their important data files, documents and pictures. Customers should also file a report with the FBI's Internet Crime Complaint Center at www.IC3.gov.

You might be asking yourself how to stay on top of the latest cyber threat tactics. The best tool in my opinion is *information sharing*. This is nothing new in the physical world. Without it, our medical field would have never left the dark ages of the eighteenth century; a time when bedside manners, ill-conceived notions of "unique illnesses," and demanding patients, prevented much headway.

The field only advanced after doctors began working together and sharing information about illnesses, diseases and remedies. The Financial Services Information Sharing and Analysis Center (FS-ISAC) is recommended by the Federal Financial Institutions Examination Council (FFIEC) and can help by providing the secure channels required – anonymized if you wish – for giving and receiving threat intelligence and indicators. Memberships start at $250/year for institutions with less than $1 billion in assets / $10 million in revenue. You might also sign up for US-CERT vulnerability advisories, FFIEC press releases and Better Business Bureau (BBB) scam alerts.

How do you protect your own financial institution from cyber threats? The National Institute of Standards and Technology (NIST), Cybersecurity Framework (CSF), specifies that a five-tiered approach works best: *identify*, *detect*, *protect*, *respond* and *recover*.

Combined with your regulatory requirement to protect information and systems from *confidentiality*, *integrity* and *availability*-related attacks, commensurate to your institution’s risk tolerance (appetite), you get an information security program able to withstand the majority of attacks.

I agree, those are a lot of generalized terms without much operational content, so it is really best to begin at the top, with an inventory of information and systems, and then perform a risk assessment.

An inventory is vital because it is nearly impossible to protect information you do not know you have. Inventory should include information and systems located in your data center and hosted elsewhere (i.e., with vendors or 3rd party providers). Review the FFIEC’s recently-updated Information Technology (IT) Examination Handbook on Management, which provides additional guidance and requirements on the processes and procedures to help mitigate risk.

If you do not already have a risk assessment, the FFIEC provides the *Cybersecurity Assessment Tool* (CAT) to help. After you read through the CAT documentation, before using it, you will want to download the *Automated Cybersecurity Assessment Tool*, a Microsoft Excel spreadsheet to apply the CAT, from the Financial Services Sector Coordinating Council (FSSCC) website.

This assessment will give you and your management and directors an Agency-approved method to identify your current inherent risk level and ensure your cyber security maturity and controls are appropriate.

Whichever assessment tool you use, you will want to outline gaps and areas requiring enhancement, and develop a roadmap for your directors for enhancing your security controls, commensurate to your institution’s risk. Add the results to your information security program risk reduction strategy and incorporate costs in your budget plan.

In the next article, I will examine key security controls and training opportunities to help mitigate the season’s increased risk, as well as offer best practices to share with customers and employees to protect their own information and your enterprise.

0 Comments SecurityCurrent 1 Login

Recommend Share Sort by Best

Start the discussion…

Be the first to comment.

ALSO ON **SECURITYCURRENT** WHAT'S THIS?

Plight of Passwords

1 comment • 10 months ago

Tod T — There are some industry initiatives underway that will alleviate the password pain. The Fast IDentity Online (FIDO) Alliance finalized …

“Personal” Email, or Government Property? Did Hillary Clinton Violate Federal Laws?

1 comment • 9 months ago

Michael Alan Aisenberg — Finally, someone who has read, understands, and explains the statute. FRA and NARA are obscure and unevenly …

Breaking the Chain

1 comment • 3 months ago

ByteMe — When you are in an environment that is "open" as you state and a perimeter is tough to enforce then the concepts of dwell time and …

A CISO Checklist: 10 Deadly Sins

1 comment • 4 months ago

Tim Kropp — Farhad - Very nice work on this article and 10 checkups to keep an organization moving in the right direction.

Subscribe Add Disqus to your site Privacy

About securitycurrent | Privacy Policy | Subscribe to our newsletter