Ransomware Attacks On Community Banks

cyber security risk management

Summary: Infamous cybercriminals caused the Colonial Pipeline breach and also hacked into three community banks within the same timeframe. Seven tips can help protect your institution, including: educating employees, limiting network exposure, backing up data, automatically updating devices, contacting the FBI if attacked, reminding customers regularly, and keeping resources handy.

Did you know that Henri Matisse's painting, "Le Bateau", was hung upside down in the MoMA for a period of time? It wasn't until a stockbroker who was quite familiar with the painting noticed this and rectified the error. That said, recent events have proven that community financial institutions (CFIs) are not too small to go unnoticed by cyber thieves.

DarkSide and Ragnar Locker are two cybercriminal groups known for hacking into systems, stealing sensitive information, and then demanding a ransom or else posting all of the information. Last month, they posted evidence of a hack into Colonial Pipeline on their sites and then they did the same to three community banks.

In the case of these banks, the evidence posted included screenshots of the banks' customer databases. The hackers demanded that the banks ante up, in order to stop them from exposing the customer information. These incidents are shocking reminders that financial institutions of all sizes are fair game to these criminals.

While ransomware attacks are not new, the pandemic shutdowns and remote work arrangements have made all financial institutions (FIs) more vulnerable to these types of attacks. Indeed, the industry experienced a 520% surge in phishing and ransomware attacks between March and June 2020, according to a report by security company Arctic Wolf.

In response to this increase and recent attacks, the federal government has stepped up its role in cybersecurity too. It issued an executive order in May providing for more sharing of threat information, modernizing federal government cybersecurity, and standardizing the federal government's response to cybersecurity incidents, among other actions.

Similarly, with current events on top of mind, law enforcement officials and cybersecurity organizations are reminding FIs what they can do to stay ahead of ransomware attacks.

1. **Educate employees.** Staff should be regularly updated on the latest threats, including warning signs and safe practices to help prevent ransomware from infiltrating the institution's system.

2. **Limit network exposure.** Only authorized users should be able to install and run software applications on network devices. Also, be sure to implement network segmentation best practices.

3. **Back up data.** Ransomware attacks prevent institutions from accessing the stolen data. So, a best practice is to store a backup of the data on a separate device or offline that can be accessed, if such an attack were to occur.

4. **Automatically update all devices used by staff.** Antivirus and anti-malware solutions should be kept up-to-date. Institutions should conduct routine scans to make sure these solutions are doing their jobs.

5. **Contact the FBI if attacked.** You can find the FBI office nearest you on the FBI field offices page.

6. **Remind customers regularly.** Don't assume that all customers are well versed in cyber risk. CFIs should regularly update their customers on the ways to stay safe. A few reminders include:

- Tell customers to not open emails or attachments they don't recognize
- Keep an offline backup of personal information
- Maintain the latest security software, web browser, and operating system and turn on automatic updates.
- Enable popup blockers

7. Keep helpful resources handy. The below resources are good ones to review on a regular basis to help prepare for cyber threats from ransomware attacks.

- BITS, the technology policy division of the Bank Policy Institute (BPI)'s resource guide
- Cybersecurity & Infrastructure Security Agency (CISA)'s alerts and tips
- FBI's Ransomware Prevention and Response for CISOs
- FinCEN's Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments

Ransomware can wreak great havoc, so it is imperative to stay on top of cyber threats. This is not a one-and-done process. Continuous monitoring of threats, educating of employees and customers, and safeguarding of systems are necessary to combat these cyber thieves and stay safe.

FASTER INTERNATIONAL PAYMENTS

As a member of SWIFT gpi, PCBB can provide you and your customers with faster international payments combined with greater transparency for enhanced security. Learn more about our international services.

ECONOMY & RATES

Rates As Of: 06/17/2021 05:31AM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg
3M	0.04	0.03	-0.05
6M	0.06	0.03	-0.03
1Y	0.07	0.03	-0.04
2Y	0.22	0.07	0.09
5Y	0.92	0.12	0.55
10Y	1.58	-0.02	0.66
30Y	2.18	-0.10	0.54
FF Market	**FF Disc**		**IORB**
0.06	0.25		0.15
SOFR	**Prime**		**OBFR**
0.01	3.25		0.04