VOTIRO

14 Lessons Learned for CISOs

from a Ransomware Survivor CIO

A fascinating cybersecurity discussion panel uncovered valuable new insights to help CISOs and their organizations be better prepared for when ransomware comes knocking at the door.

Votiro and SecuLore Solutions recently hosted the panel event "Lessons Learned for CISOs from a Ransomware Survivor CIO," moderated by Tom Field, SVP Editorial at Information Security Media Group. The discussion centered around the experiences of Frank Johnson, former Public Sector CIO and Battle-Tested Ransomware Survivor. Frank now provides cyber thought leadership and best practices as an ambassador of the Cybersecurity Collaborative and Senior Vice President at SecuLore Solutions. The discussion also included Chris Fedde, Board Member of Votiro, a cybersecurity company that proactively sanitizes files of all malware and other file-borne threats without interrupting business. The Votiro Positive Selection process results in completely clean files and full file usability and functionality.

To set the tone of the event, Frank quotes the great Mike Tyson, "Everybody has a plan until they get punched in the mouth."

> *"Everybody has a plan until they get punched in the mouth."*
>
> *- Mike Tyson*

No matter how prepared you may think you are, you're most informed when you are actually struck. With this in mind, Frank focuses on using his experiences being "punched" by malware to help other CISOs improve their organization's cybersecurity standing.

Here are the 14 lessons for CISOs to learn from a Ransomware Survivor CIO:

1. Beware of ransomware's new targeted strategies

Ransomware strategy has changed drastically in recent years. Not that long ago, the strategy used by ransomware attackers was a widescale, low value attack. They would cast a wide net —often via an automated campaign — that reached a large number of victims and demanded small amounts, such as $1K to $5K in exchange for ransomware recovery. According to Chris Fedde, that's not what we're seeing now. Now the modus operandi is pinpoint attacks against high value targets, and the attackers are not looking for $5,000 anymore. Instead, it's $5,000,000. Early phishing activities against vaccine makers have already been detected.

> **"We all remember not long ago, not long ago at all, when the strategy was a broadcast commodity kind of attack, large numbers, automated $5,000 here, $1,000 there. And it was very much a strategy of cast a wide net, get lots of victims, small victims, and it rolls up to a lot of damage.**
>
> **That's not what we're fighting now. That's not what we're seeing now. Now it's targeted attacks, targeted attacks against high value targets. A human being is behind the attack, and they're not looking for $5,000 anymore. It's $5,000,000. That's not an exaggeration, lots of examples today of $1,000,000 ransoms, $5,000,000 ransoms against these high value targets."**
>
> **- Chris Fedde, Board Member, Votiro**

2. Lightning-speed malware techniques move faster than you can

Malware techniques have greatly improved. The time lapse from when they breach the network until they're ready to encrypt is no longer weeks or months. It's now hours. With these short dwell times, companies have very little time to detect and respond, especially considering that these attacks are not generating very much digital noise on the network. These advanced attacks are fairly quiet and feature clean URLs. They're not tripping anomaly detectors and are not always seeking to exfiltrate. By the time you are ready to react, you have already become a statistic.

Bottom line: you're not going to be effective in fighting the ransomware attackers, so you must prevent it by keeping them from ever getting past the front door.

3. Even the best training isn't sufficient

Your weakest link is always your user base, so training and awareness are very important. Employees must be trained to watch out for phishing, what not to click on, and the importance of patching. **However – and we all know this - if your first line of defense is dependent on a person — on human error — you're at a disadvantage against the attacker.** Though training will reduce the organization's susceptibility to a breach, it will never result in 100% coverage as there will always be user error. While awareness is important, reliance on technologies is a safer bet for preventing ransomware.

4. Leadership must carry the cybersecurity burden

It should not be left up to the IT organization to determine risk profile or to appeal for more cyber resources through the budgeting process. Leadership — whether defined as public or private — must be responsible for the high level, top-down strategic planning. The level of investment required to lower organizational risk should be informed by a formal risk assessment. Unfortunately, few organizational leadership teams put in the effort necessary to protect digital assets and fight ransomware.

5. Effective cybersecurity relies on soft skills

Frank explains that cybersecurity is not a technological issue, rather it is 100% a people issue. His advice for CISOs is to focus on the soft skills. Forget about your brilliance, tech know-how, or certifications. None of that matters when it comes to advocating for the budget needed to protect the network or hire new resources. As a cybersecurity leader, you need to be a true collaborator and a great influencer. You have to help inform the budget. You've got to show up at the board room.

6. Beyond incident response, communication is most important

Frank emphasizes the importance of communication, communication, communication. CISOs have a responsibility to keep leadership, internal customers, partners, constituents, and sometimes even local municipalities, informed. Don't be afraid to engage professional expertise in helping you manage the message and get the word out to key audiences.

Watch the Event

Lessons Learned for CISOs from a Battle-tested, Ransomware Survivor Public Sector CIO

7. The largest piece of the ransomware recovery budget goes to personnel resources

When your organization experiences a breach, you want to quarantine the incident and get online as quickly and safely as possible — but you will need help. Most organizations do not keep this level of resources on staff, and rightly so. As an analogy, most companies do not keep firefighters on staff to be prepared in case of a fire. You bring in the experts, if and when necessary. These on-demand resources are not inexpensive, so that's where most of your recovery budget will go. Some additional expenditures will be needed to help you prepare against future ransomware attacks.

> **"Most of the dollars spent go to resources to help you do those two functions, resources that you do not - and probably should not - keep on staff because you can't afford to. You don't need firefighters every single day, you need operators. So you spend your scarce resources on keeping systems running, not a team of firefighters sitting in the corner, waiting for the building to catch on fire. When something happens, you bring them in. They're not inexpensive, they're in demand."**
>
> **- - Frank Johnson, SVP, SecuLore Solutions**

8. Paying the ransom does not speed up recovery

If you are tempted to just pay the ransom thinking you will get the key, un-encrypt the systems, and throw your network back into production, don't. Not only would that be reckless, but paying the ransom does not speed up your recovery. Putting systems back online safely and securely is your priority, and you can't circumvent that process. Download the backup, check it for indicators of compromise, add more cyber capability, and hand it over to the system administrator so they can go do their regression. After user testing, carefully put it back into the relevant environment and slowly start to add users. There is no way around the process. Aside from all that, the federal authorities all strongly recommend against paying the ransom.

9. Take incident response planning seriously

Frank quotes philosophers who have said, "You cannot control what happens to you in life, but you can control 100% of the time how you respond to it." Be as prepared as possible by having a well-thought-out incident response plan that you practice, no different than a fire drill. When an incident occurs — not if — everyone will know what to do: coolly, calmly, and as efficiently as possible. Keep in mind that good corporate cyber hygiene today dictates that you should have an independent third party providing that cybersecurity incident response planning.

10. Your cyber insurance provider may have a preferred incident response plan

If you're fortunate enough to have cybersecurity insurance, your underwriter will typically have a preferred incident response vendor that they want you to work with on the best way to resolve a ransomware threat. Meet that team ahead of time, get to know them, and determine key SLAs so when there's an incident, so there are no surprises.

11. Backups need to be close & accessible at all times

If you think you don't have to worry because you have good backups, think again. Most cyber criminals are in your environment well before you discover them, so your backups may be corrupted or full of indicators of compromise. Make sure your backups are kept close by —maybe even in your own production environment — so that you can gain access right away.

Frank gives a descriptive analogy, "Trying to download petabytes of information through a one gig pipe is like sucking air through a straw on top of Mount Everest." He means that when you start the process of recovery post-incident, you need that information back on the prem as quickly as possible, so keep that in mind when considering your ransomware backup strategy.

> **"Trying to download petabytes of information through a one gig pipe is like sucking air through a straw on top of Mount Everest."**
>
> **- Frank Johnson, SVP, SecuLore Solutions**

12. Cloud is key

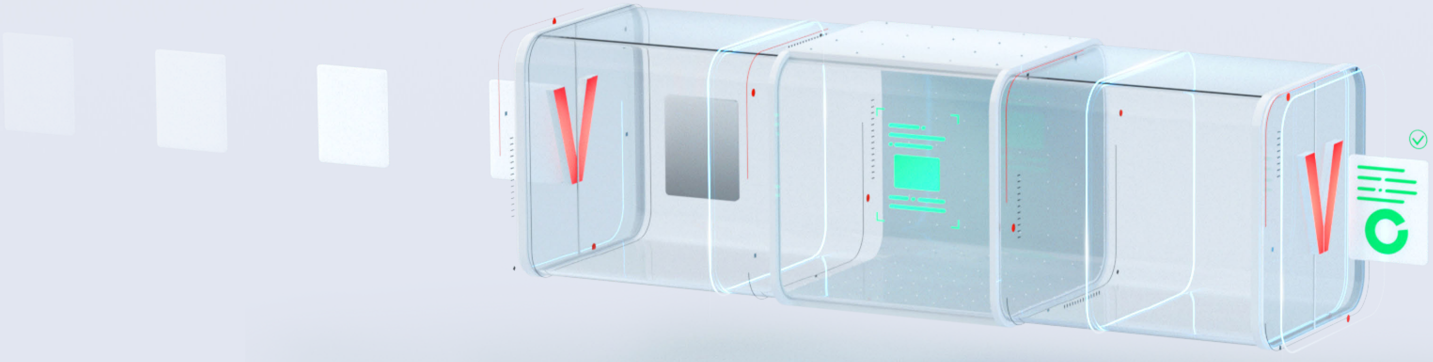
Are you wondering whether your assets are safer in the cloud than they are on prem? If you are fortunate enough to be in a major IT operation with massive IT budgets and significant security teams with lots of sophisticated tools and capability, you'll probably argue that you're better off on prem. But the rest of us — 80 to 90% of the market — armed with a handful of cyber professionals (if you're lucky) cannot possibly fend off the global cyber-crime industry. Your assets will likely be safer at a large hyperscaler who has an army of cyber professionals and spends millions of dollars on cyber protection. Keep in mind that you can still smartly diversify your cloud portfolio as most of these large hyperscalers can diversify your capability assets within their large environments.

13. Work out your contracts with vendors ahead of time

Your vendors will play an important role in your cyber response. Keep in mind that when an incident occurs, these vendors will largely go unnamed even though infrastructure was compromised utilizing their tools and capabilities. You must have clear contracts worked out with how fast they will respond when you pull the fire alarm. Some vendors will drop everything and run to your aid. Others will require T's and C's and documents to be signed. Work out contracts ahead of time to clarify your true partners in fighting ransomware.

14. Being a ransomware survivor puts you ahead of the curve

Once upon a time, a CISO hit with ransomware may have felt like they were walking around in society with a scarlet letter stamped on their forehead, and a potential employer wouldn't touch them with a 10-foot pole. But today, ransomware is so prevalent in IT that many employers would prefer to hire someone battle-tested, who has lived through a ransomware attack. Living through a cybersecurity event gives you the skills and experience that you would never garner elsewhere.



Preventing Ransomware, Instead of Detecting & Responding

Chris rounds out the discussion by explaining that ransomware almost always enters a network using weaponized content — usually emails. And that's where Votiro's technology comes into play.

Unlike detection-based file security solutions that scan for suspicious elements and block some malicious files, Votiro Cloud's Positive Selection technology allows through only the safe elements of each file, ensuring every file that enters the organization is 100% safe. So, by ensuring that only safe content is delivered to the network, you effectively eliminate the method that ransomware utilizes in their attacks. Although this technology wasn't available to Frank when his organization was attacked, it is available now.

To learn more about Votiro's innovative approach to cybersecurity, click here.

To learn more about SecuLore Solutions, click here.

Watch the Event

Lessons Learned for CISOs from a Battle-tested, Ransomware Survivor Public Sector CIO

Chris Fedde
Board Member, Votiro

Chris Fedde is a Board Member at Votiro, a cybersecurity company that sanitizes files of malware and other embedded threats while maintaining full file usability and functionality. Previously, Chris Fedde served as the CEO of Bandura Cyber, Inc, leading the company through its early growth in cyber threat intelligence while raising two institutional capital raises. Prior to Bandura, Mr. Fedde founded and led Hexis Cyber Solutions, Inc, which was acquired in 2016.

Prior to Hexis, he was president and Chief Executive Officer of SafeNet, Inc., a global leader in data protection. SafeNet was sold to Gemalto in 2014. Mr. Fedde currently serves on the boards of Votiro Cybersecurity, Netcraftsmen, and other technology firms and non-profits, as well as advisory boards of tech companies. Mr. Fedde holds several technology patents.

Frank Johnson
SVP, SecuLore Solutions

Frank Johnson previously served as a City Chief Information Officer (CIO) and Chief Digital Officer (CDO). Frank was charged with leading and supporting all digital transformation programs and efforts to modernize the City’s IT capabilities, scale the local IT ecosystem and drive awareness/tech investment to the city.

As a former “ransomware battle-tested” CIO, he is now focused on helping others in all aspects of cybersecurity by providing cyber thought leadership and best practices as an Ambassador of the Cybersecurity Collaborative and SVP at SecuLore Solutions.

Experience Secure Files For Yourself

Schedule A Demo

About

Votiro

Votiro Cloud is the only solution that guarantees complete protection from weaponized files. Unlike detection-based file security solutions that scan for suspicious elements and block some malicious files, Votiro's revolutionary Content Disarm and Reconstruction technology singles out only the safe elements of each file, ensuring every file that enters your organization is safe.

Founded by leading file security experts, Votiro's new approach to file security works invisibly in the background, completely eliminating threats while ensuring zero interruption to business. Votiro is trusted by large enterprises globally, including top Fortune 500 companies, to completely eliminate file-based threats while ensuring business continuity. Headquartered in the United States, with offices in Australia, Israel and Singapore, Votiro is trusted by over 2 million users worldwide to safely access and recieve files with complete peace of mind.

Contact Votiro

info@votiro.com
votiro.com