# Holidays and Weekends: Prime Time for Cyberattacks

by Sharon D. Nelson, Esq., John W. Simek and Michael C. Maschke



**Did Your Law Firm Survive Thanksgiving?**

We're happy to say that our company survived – but we were attacked over 400 times between shutting the office down on Wednesday evening and Thursday morning. All of the attacks originated from Microsoft IP addresses (are you addressing this Microsoft?).

Did we get a good night's sleep that Wednesday? Sure. Good preparation for attacks means that, if the attack is unsuccessful, you don't get alerts. We learned of all the attacks first thing Thanksgiving morning, with a full report to review over our morning coffee.

Don't think we're cocky about "winning" the battle. No one is immune from cyberattacks, no matter how good their defenses are. We regard it as being both well prepared – and lucky.

But it did occur to us, with Christmas and New Year's on the way, that it was time to underscore to law firms something that should be obvious: Cybercriminals don't go on holiday!

**Shore Up Your Law Firm Defenses: Scary Stats**

The week before Thanksgiving, cybersecurity firm Cybereason published the results of its recent survey. Understandably, more than a third of respondents reported that it took longer for their organization to assess, stop and recover from a cyberattack on a holiday or weekend attack as opposed to a weekday. The larger the organization, the longer the delay.

They also lose more money because of those attacks, which are primarily ransomware attacks. The root of the problem is that so many victims are understaffed on weekends and holidays. Half of respondents reported being staffed at levels below 33%. 20% of companies cut security staffing by 90% from normal weekday levels.

This gives attacks more time to avoid detection, do more damage and exfiltrate more data as these understaffed security teams scramble to respond.

**Cyber Pros Buckle Up, Worried About a Visit from The Grinch**

It has now been a lot of years that cyber pros have been battling holiday-related attacks, so most of them on edge – and lacking the power to demand that staffing be maintained at normal or close to normal levels.

When Santa comes this year, all these experts know that hackers will not be far behind. History is our guide: From the Aurora attacks on Google in 2009 to the more recent Log4J and SolarWinds attacks, the notable fact is that these attacks took place mostly between Thanksgiving and New Year's Day.

No cyber pro worth his or her salt assumes they will be home for the holidays.

**A Gift of Ransomware for the Holidays?**

Yeah, not much of a gift, but once that seems to be ever-increasing. In 2021 there was a 70% increase in ransomware attacks in November and December compared to January and February.

So, what is a law firm to do? The best advice these days comes from the Cybersecurity and Infrastructure Security Agency (CISA), part of the Department of Homeland Security. Its advice, well worth taking, has been updated for 2022.

Here are, verbatim, some of the tips that are integral to preventing and fighting weekend and holiday attacks. Law firm management should make sure all of these steps are in place.

*"Understand the IT environment's routine activity and architecture by establishing a baseline. By implementing a behavior-based analytics approach, an organization can better assess user, endpoint, and network activity patterns. This approach can help an organization remain alert on deviations from normal activity and detect anomalies. Understanding when users log in to the network—and from what location—can assist in identifying anomalies. Understanding the baseline environment—including the normal internal and external traffic—can also help in detecting anomalies. Suspicious traffic patterns are usually the first indicators of a network incident but cannot be detected without establishing a baseline for the corporate network.*

- *Review data logs. Understand what standard performance looks like in comparison to suspicious or anomalous activity. Things to look for include:*
    - *Numerous failed file modifications,*
    - *Increased CPU and disk activity,*
    - *Inability to access certain files, and*
    - *Unusual network communications.*
- *Employ intrusion prevention systems and automated security alerting systems—such as security information event management software, intrusion detection systems, and endpoint detection and response.*
- *Deploy honeytokens and alert on their usage to detect lateral movement.*

*Indicators of suspicious activity that threat hunters should look for include:*

- *Unusual inbound and outbound network traffic,*
- *Compromise of administrator privileges or escalation of the permissions on an account,*
- *Theft of login and password credentials,*
- *Substantial increase in database read volume,*
- *Geographical irregularities in access and log in patterns,*
- *Attempted user activity during anomalous logon times,*
- *Attempts to access folders on a server that are not linked to the HTML within the pages of the web server, and*

- *Baseline deviations in the type of outbound encrypted traffic since advanced persistent threat actors frequently encrypt exfiltration."*

**Final (Altered) Words from The Grinch Whole Stole Christmas**

*I must stop Christmas from coming... but how? He puzzled and puzzled 'till his puzzler was sore. Ransomware, that's how!*

***Sharon D. Nelson*** *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA. snelson@senseient.com*

***John W. Simek*** *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm. jsimek@senseient.com.*

***Michael C. Maschke*** *is the CEO/Director of Cybersecurity and Digital Forensics of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744) a Certified Ethical Hacker and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional. mmaschke@senseient.com.*