AN A.S. PRATT PUBLICATION
MAY 2022
VOL. 8 NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 8 **NUMBER 4** **May 2022**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [8] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [113] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2022–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Capping Cyber Casualties: Steps to Avoid Cyberattacks Flowing from Hostilities in Ukraine

By Paul H. Luehr, Kenneth Dort, David W. Porteous, Jason G. Weiss, Peter W. Baldwin, Doriann H. Cain, Kathryn R. Allen, Mitchell S. Noordyke and Jane E. Blaney*

Recognizing that cyberattacks have already commenced and could spread beyond the Russian-Ukrainian battlefield, the authors of this article discuss the risks and how organizations can protect themselves.

The televised "thud" of explosions in Ukraine has an ominous but deceptively distant tone. For many organizations the hostilities are closer at hand, in the form of cyberattacks that could spread beyond the Russian-Ukrainian conflict. The Federal Bureau of Investigation ("FBI") has already warned businesses, banks and local governments about the increased risk of cyberattacks, and the Cybersecurity & Infrastructure Security Agency ("CISA") within the U.S. Department of Homeland Security has issued a "Shields Up"[1] warning to counter possible Russian attacks. We should take these warnings seriously. Cyber warfare has already begun.

Many Ukrainian banks and government departments have already gone dark; and the Ukrainian internet company NetBlocks has suffered a Distributed Denial of Service ("DDoS") attack. Meanwhile, a new malicious "wiper" program has been unleashed to destroy infected machines.

HISTORY

We can learn from history because we have seen this all before. Current cyber assaults mimic earlier DDoS attacks attributed to Russia during its 2008 and 2014 incursions into Georgia and the Crimea. The new "wiper" program also resembles the NotPetya malware that wreaked havoc around the world in 2017 and 2018.

NotPetya was a virus originally found in Ukrainian accounting software, which had been modified to encrypt targeted systems. The Central Intelligence Agency ("CIA") concluded that Russia had deployed NotPetya as a cyber weapon to cripple Ukraine's financial system. Unfortunately, NotPetya spread far beyond the Ukraine, infecting

* Paul H. Luehr (paul.luehr@faegredrinker.com), Kenneth Dort (kenneth.dort@faegredrinker.com), David W. Porteous (david.porteous@faegredrinker.com), Peter W. Baldwin (peter.baldwin@faegredrinker.com) and Doriann H. Cain (doriann.cain@faegredrinker.com) are partners at Faegre Drinker Biddle & Reath LLP. Jason G. Weiss (jason.weiss@faegredrinker.com) is counsel and Kathryn R. Allen (kathryn.allen@faegredrinker.com), Mitchell S. Noordyke (mitchell.noordyke@faegredrinker.com) and Jane E. Blaney (jane.blaney@faegredrinker.com) are associates at the firm.

[1] https://www.cisa.gov/shields-up.

Windows servers, PCs and laptops throughout the world. Originally thought to function like generic ransomware with a key, a devastating version of NotPetya had no key and could not be decrypted, transforming the program into a pure form of "disruptionware," also known as a "wiper." It took down global shipping firms, food companies and even law firms. By the end of 2018, the estimated damage caused by NotPetya exceeded $10 billion worldwide.

WHAT CAN ORGANIZATIONS DO?

To avoid a repeat of this devastation, and as explained in more detail below, organizations can take the following actions to better protect themselves against new cyberattacks:

1. Assess your risk;
2. Upgrade and test backups;
3. Practice your incident response plan;
4. Block unwanted traffic;
5. Implement multi-factor authentication ("MFA");
6. Patch Log4j vulnerabilities; and
7. Check your cyber insurance policy.

ASSESS YOUR RISK

Cybersecurity is most effective when organizations realistically assess their vulnerabilities and threats, the damage they could cause, and the likelihood of such harm. Many analysts put this risk in mathematical terms. For cybersecurity, we think the best equation is: Risk = Threats x Vulnerabilities x Harm x Likelihood.

Here, the most realistic threats are "wiper" programs gone rogue, or DDoS and ransomware attacks targeting institutions closely associated with American democracy and culture. These institutions would include local, state and federal agencies, as well as organizations with strong brands that evoke images of blue jeans, rock 'n roll, fast cars, faster computers or just "Mom, baseball and apple pie." From historic conflicts, we know attackers will target some companies, unfortunately, merely because they include "U.S." or "America" in their names.

Beyond these external threats, organizations also should assess their own vulnerabilities. Do they have good daily backups, effective patching procedures and secure vendors? If not, now is the time to build or improve these security measures, otherwise the likelihood and harm of an attack may be amplified.

Finally, an effective risk assessment should play out worst-case scenarios. If a new NotPetya virus hits our systems, what would fail? What would survive? Could we operate the factory floor without internet connectivity? Would remote workers at home be locked out? For how long?

Addressing these "what if" questions will help your organization establish clear priorities and better contingency plans.

UPGRADE AND TEST BACKUPS

Many cybersecurity experts believe it is unrealistic to block all cyberattacks. They often say, "The question is not if, but when, you will be attacked." From this perspective, resilience should be an organization's main goal, and effective data backups and restoration are critical.

The National Institute of Standards and Technology ("NIST") has outlined best backup practices in a document called "Protecting Data From Ransomware and Other Data Loss Events."[2] When creating a backup plan, NIST recommends several steps, including the following:

- Narrowly define the most critical information to back up and restore in a crisis.
- Identify regulatory and legal data retention requirements, with specific care for customer files and other custodial obligations.
- Determine the restoration time for different types of data, accounting for internet bandwidth, offsite facility bandwidth, and file or hardware transfer rates.
- Understand any dependencies and the required order of restoration.
- Determine workplace relocation options to ensure business continuity.
- Secure mission-critical data offline, including passwords, digital certificates and encryption keys needed for data restoration.

2 https://www.nccoe.nist.gov/sites/default/files/legacy-files/msp-protecting-data-extended.pdf.

- When possible, follow the 3-2-1 rule:
    - 3 – Keep three copies of any important file: one primary and two backups.
    - 2 – Keep files on two different media types to protect against different hazards.
    - 1 – Store one copy – or "go bag" – off-site (e.g., outside the home or office).
- Test the plan for recovery, and verify:
    - Backup file integrity;
    - Speed and efficiency of recovery;
    - Roles and responsibilities; and
    - Time to restore files and rebuild systems.

PRACTICE YOUR INCIDENT RESPONSE PLAN

Your backups are just one key aspect of your overall incident response plan. With the threat of new cyberattacks looming, we recommend dusting off your full incident response plan to ensure your organization can promptly and effectively respond. As you conduct a review of your incident response plan, ask the following questions:

- Are the procedures easy to follow?
- Does the plan account for recent changes to data privacy and cybersecurity laws?
- Does the plan account for changes in our operations, internal structure or staffing?
- Does the plan account for new software applications, cloud services, detection tools or other changes in technology across our organization?
- To implement the plan, do we need to do more employee training?

To ensure your incident response plan is working as designed, it is important to not only review the plan, but also test it. For example, conduct a tabletop exercise to make sure everyone knows their role and understands the new types of threats presented by the Ukrainian crisis. Performing this exercise will improve your organization's plan and help you build true resilience.

BLOCK UNWANTED TRAFFIC

To address new potential threats originating from the Ukraine or Russia, organizations can try to block or isolate internet traffic from that region of the world. Of course, sophisticated attackers can use anonymous routers and third-party "jump" points to reach your servers, but organizations that only do business in the United States can still minimize cyberattacks by blocking all foreign internet protocol ("IP") addresses. If some international traffic must be allowed based on supply-chain needs or overseas contacts, organizations can "whitelist" trusted IP addresses and still block foreign IP ranges not needed for daily operations.

Also, organizations can funnel internet traffic through trusted network gateways. Most legitimate internet traffic flows through designated TCP/IP protocols or channels called "ports." Therefore, your IT manager can help protect your organization by allowing appropriate traffic through common ports like 25 (email), 53 (DNS), 80 (web traffic), and 443 (secure web traffic), but blocking or disabling 65,000+ other ports that are not needed. These may include ports 22 (secure shell) and 3389 (remote desktop protocol ("RDP")), which many attackers have used to gain recent footholds on targeted networks.

Finally, organizations can take measures to prevent DDoS attacks like those seen in past Russian-Ukrainian conflicts. DDoS attacks try to overwhelm and shut down organizations by overwhelming their websites or servers with worthless traffic. These attacks are fairly easy to thwart if an organization recognizes junk traffic at the far edge of its network and then blocks that traffic or sends it to a dead address called a "black hole." Many cloud and internet service providers will provide this type of perimeter monitoring or "blackholing," so ask your IT professionals if your organization subscribes to such services.

IMPLEMENT MULTI-FACTOR AUTHENTICATION

If attackers manage to defeat your IP blocking or perimeter defenses, an effective last line of defense is MFA. MFA works on the principle that a valid user can only enter a network if they present "something they know" (like a username and password) and "something they have" (like a signal from a mobile authentication app or a code just sent via SMS text). Even if an attacker "knows" an employee's online credentials through a previous theft or hack, MFA reduces the risk that the credentials can be used illegally to access an organization's network because the hacker does not "have" the second key – namely the mobile app or SMS code.

According to NIST,[3] MFA is a critical stop-block that "can massively reduce the likelihood you'll be the next victim." Many cyber insurers now require a covered organization to implement MFA, so if you do not have MFA currently, you likely will in the near future. We recommend implementing MFA now. Otherwise, you may need to implement MFA in a time of crisis during an actual breach. This could require you to hire expensive contractors to work on MFA while your IT department stays focused on stopping the attack. In short, MFA can limit the success of a new cyberattack and help give piece of mind during these stressful times.

PATCH LOG4j VULNERABILITIES

Apart from addressing external threats, organizations also should reduce their internal vulnerabilities. Today, that often means addressing the recent Log4j vulnerability. It is not the only vulnerability that organizations need to remedy, but Log4j has been leveraged in many recent attacks.

In December 2021,[4] the information security industry identified the "Log4j" or "Log4Shell" vulnerability (CVE-2021-44228,[5] CVE-2021-45046[6] and CVE-2021-45105[7]), a new "zero day" vulnerability that allowed hackers to exploit a critical remote code execution ("RCE") in the Apache Log4j library. This library is commonly used by programmers to build enhanced logging functions into Java-based software applications. The Log4j utility is so ubiquitous that many organizations may not be aware it is built into many software programs they use daily. The vulnerability allows attackers to: (i) trick an application into leaking sensitive information, and (ii) remotely upload and execute malicious code. After the Log4j vulnerability was announced, it took less than a month[8] for the vulnerability to become the most prevalent means used to launch cyber intrusions.

In light of the increased risk of cybersecurity attacks emanating from Russia or Russian-affiliated threat-actor groups, organizations should follow the mitigation steps jointly outlined by international agencies,[9] including CISA, the FBI and the National Security Agency ("NSA"), to address the Log4j vulnerability.

---

[3] https://www.nist.gov/blogs/cybersecurity-insights/back-basics-whats-multi-factor-authentication-and-why-should-i-care.

[4] https://www.discerningdata.com/2021/discerning-data-cyber-vulnerability-alert-log4j/.

[5] https://nvd.nist.gov/vuln/detail/CVE-2021-44228.

[6] https://nvd.nist.gov/vuln/detail/CVE-2021-45046.

[7] https://nvd.nist.gov/vuln/detail/CVE-2021-45105.

[8] https://www.globenewswire.com/news-release/2022/02/23/2390470/0/en/FortiGuard-Labs-Reports-Ransomware-Not-Slowing-Continues-to-be-Relentless-and-More-Destructive.html.

[9] https://www.cisa.gov/uscert/ncas/alerts/aa21-356a.

Such mitigation steps include the following:

- *Identify vulnerable assets in your environment*. Inventory all applications that use the Log4j Java library and identify those versions that are likely to be vulnerable.
- *Mitigate known and suspected vulnerable assets in your environment*. Patch Log4j and other affected products to the latest version, keep an inventory of those assets and actions taken, and verify that the mitigation was successful.
- *Initiate hunt and incident response procedures*. Hunt for signs of exploitation and compromise. If detected, follow appropriate response procedures. Report compromises to the authorities.
- *Evaluate and apply other mitigation*. Continue to monitor the Apache Log4j Security Vulnerabilities[10] webpage for new updates. Block any suspect outbound Log4j network traffic.

In addition, refer to the following resources to help identify and mitigate vulnerable assets:

- CISA's Log4j scanning tool,[11] which can identify vulnerable Log4j hosts.
- CISA's additional guidance[12] and list of affected and unaffected software by vendor.
- The National Cyber Security Center in the Netherlands's ("NCSC-NL") list of affected and unaffected software.[13]

CHECK YOUR CYBER INSURANCE POLICY

Apart from accepting, preventing or mitigating risk, many organizations believe they can transfer the risk of cyberattacks through insurance. These organizations carry cyber insurance but probably only possess a vague notion of what their policy covers. Now is the time to check, especially in light of the controversy that swirls over "act of war" insurance exclusions.

[10] https://logging.apache.org/log4j/2.x/security.html.
[11] https://github.com/cisagov/log4j-scanner/tree/master/log4-scanner#features.
[12] https://github.com/cisagov/log4j-affected-db.
[13] https://github.com/NCSC-NL/log4shell/blob/main/software/software_list_0-9.md.

A recent "real world" case highlights the issue. In *Universal Cable Prods., LLC, et al. v. Atl. Specialty Ins. Co.*,[14] Universal Cable Productions, a unit of NBCUniversal, sought recovery when it had to move its production out of Jerusalem after rockets were fired into Israel by Hamas. The insurer denied this claim, citing the policy's "act of war" exclusion. The court ultimately found that the rocket attacks were not acts of war and that the insurer breached its contract by denying the studio's claim. The insurance policy "excluded coverage for expenses resulting from 'war,' 'warlike action by a military force,' or 'insurrection, rebellion, [or] revolution.'" In the insurance context, the court held an act of war requires "the existence of hostilities between de jure or de facto governments." The court found that Hamas was neither, noting that the executive branch had refused to recognize it as a sovereign power.[15]

A similar cyber insurance case is now wending through the courts. The case arose out of the NotPetya cyberattack described above. Among others, the food giant Mondelez was injured, incurring more than $100 million in damages. When Mondelez filed a claim under its cyber insurance policy, coverage for this attack was denied under the insurer's "act of war" exclusion, because NotPetya was considered a "hostile or warlike action" by a "government or sovereign power." Mondelez brought suit against the insurer for breach of contract, promissory estoppel, and vexatious and unreasonable conduct. This case is still pending in Illinois.

As these cases illustrate, insurance coverage may not be guaranteed for a cyberattack that originates from Ukraine. Coverage may hinge on whether the attack uses malware designed for military purposes or whether the perpetrators (e.g., Ukrainian rebels or Russian-sponsored criminals) are sufficiently aligned with a sovereign state to call their activities an "act of war."

CONCLUSION

Overall, these are fraught times, but organizations can do more than wring their hands. Recognizing that cyberattacks have already commenced and could spread beyond the Russian-Ukrainian battlefield, organizations can take several steps to protect themselves. They can recognize the risk. Then organizations can assess likely cyber threats and vulnerabilities, build resilience and take preventive actions, to avoid becoming another casualty in a conflict that already has too many.

---

[14] 929 F.3d 1143 (9th Cir. 2019).

[15] *Universal Cable Prods.*, 929 F.3d at 1154; *see Oetjen v. Cent. Leather Co.*, 246 U.S. 297, 302, 38 S. Ct. 309, 62 L. Ed. 726 (1918).