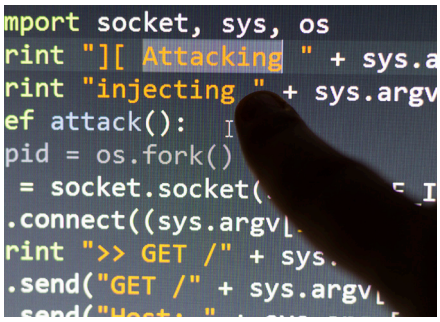
BakerHostetler

Ransomware: Prevention & Preparation



10% of the **450+** security incidents BakerHostetler led clients through in 2016 involved ransomware.

Source: 2017 BakerHostetler Data Security Incident Response Report

24 hour toll-free Data Breach Hotline **855.217.5204**

Ted Kobus quoted by *LegalTech News*, July 3, 2017: "If you're dealing with a ransomware issue and your email is down, the last thing you want to do is get on the phone with an attorney or service provider who says, 'We should get you on another provider.' You want a provider who says, 'Here's another [email] solution, and it's compliant with HIPAA, and we can get you on it in 20 minutes.'"

Recent media reports have covered "cyberattacks" involving ransomware variants that have had widespread impact on companies, including shutting down business operations.

Based on our experience leading clients through thousands of security incidents, we recognized that these new ransomware outbreaks require more than a cookie-cutter response. To provide the service our clients need to effectively respond to the mix of data security, compliance and business continuity issues caused by these outbreaks, BakerHostetler established a Ransomware SWAT Team. This is a cross-disciplinary team that includes members from our privacy and data protection, e-discovery advocacy and management, and healthcare teams.

Key issues we help clients navigate include:

- Access to key strategic advisors, including data forensic and cybersecurity companies
- Communications with regulators
- Addressing patches and risk assessment practices
- Obtaining a funded bitcoin wallet to pay ransom
- Serving as an information repository during widespread incidents and sharing accumulated knowledge (threat information sharing)
- Preserving crucial evidence
- Engaging law enforcement at the highest levels for support
- Establishing compliant offline communications when systems are down
- Leveraging downtime processes from business continuity and disaster recovery plans
- Working with company boards to remain focused on restoring services, fulfilling legal obligations, and developing communications for internal and external parties

Top Tips

Establish and fund a bitcoin wallet. We evaluate on a case-by-case basis whether or not to pay the ransom demand, which often requires payment with a very short turnaround time – sometimes barely or not long enough to establish a bitcoin wallet. We recommend that companies consider establishing and funding a bitcoin wallet well before they need one.

Contain and isolate affected systems. The modus operandi of ransomware is to encrypt all data accessible from the point of infection, both locally and over the network. Therefore, when you identify an incident involving ransomware, you should take steps to immediately contain and isolate affected systems from the network instead of unplugging the power cord.

Preserve the ransomware and encrypted data. Your first instinct may be to run antivirus software to scan and remove all traces of the ransomware from your systems. But use caution, because doing so may destroy relevant evidence. You should preserve the ransomware, encrypted data and any available network logs. If you do not have the internal expertise, consider engaging a forensic investigation firm to handle this aspect of the investigation. Security researchers have been able to crack the encryption used by some variants; however, this is a rare exception that sometimes takes years, so don't rely on this as part of your incident response plan.

Analyze the ransomware. While most ransomware operates the same way, some have different features and capabilities. For example, some ransomware is deployed along with other malicious code, while other variants are manually installed by hackers who have breached your network. Knowing the exact variant will help your outside counsel or breach coach advise you on possible notification obligations and forensic investigation next steps.

Restore access to systems. After the ransomware and related evidence have been preserved, you can take steps to restore access to affected systems and data, typically by restoring from a backup. Consult with your forensic investigator and/or breach counsel to determine if re-imagining the system or using standard removal tools is sufficient to address the variant of ransomware you are facing.

Perform a post-incident assessment. After the incident has been contained and access has been restored to affected systems, consider conducting a post-incident assessment. Do additional technical safeguards need to be implemented? Did the backup routines successfully restore critical data and systems within an acceptable time period? These questions can help improve the security of your systems and help prevent and/or minimize the impact of a similar incident in the future. Finally, compare your response with your incident response plan to identify areas needing improvement, and consider performing a tabletop exercise to reinforce the lessons learned from this incident.

Our Ransomware SWAT Team

Theodore J. Kobus III
Partner
Leader, Privacy and Data Protection Team
+1.212.271.1504
tkobus@bakerlaw.com

David M. Brown
+1.215.564.2862
davidmbrown@bakerlaw.com

Erich M. Falke
+1.215.564.6529
efalke@bakerlaw.com

Randal L. Gainer
+1.206.332.1381
rgainer@bakerlaw.com

May Tal Gongolevsky
+1.212.589.4213
mgongolevsky@bakerlaw.com

Edward J. Jacobs
+1.212.589.4674
ejacobs@bakerlaw.com

Scott Koller
+1.310.979.8427
mskoller@bakerlaw.com

Stephanie A. Lucas
+1.310.442.8847
slucas@bakerlaw.com

Lynn Sessions
+1.713.646.1352
lsessions@bakerlaw.com

bakerlaw.com

Recognized as one of the top firms for client service, BakerHostetler is a leading national law firm that helps clients around the world to address their most complex and critical business and regulatory issues. With five core national practice groups – Business, Employment, Intellectual Property, Litigation and Tax – the firm has more than 940 lawyers located in 14 offices coast to coast. For more information, visit bakerlaw.com.