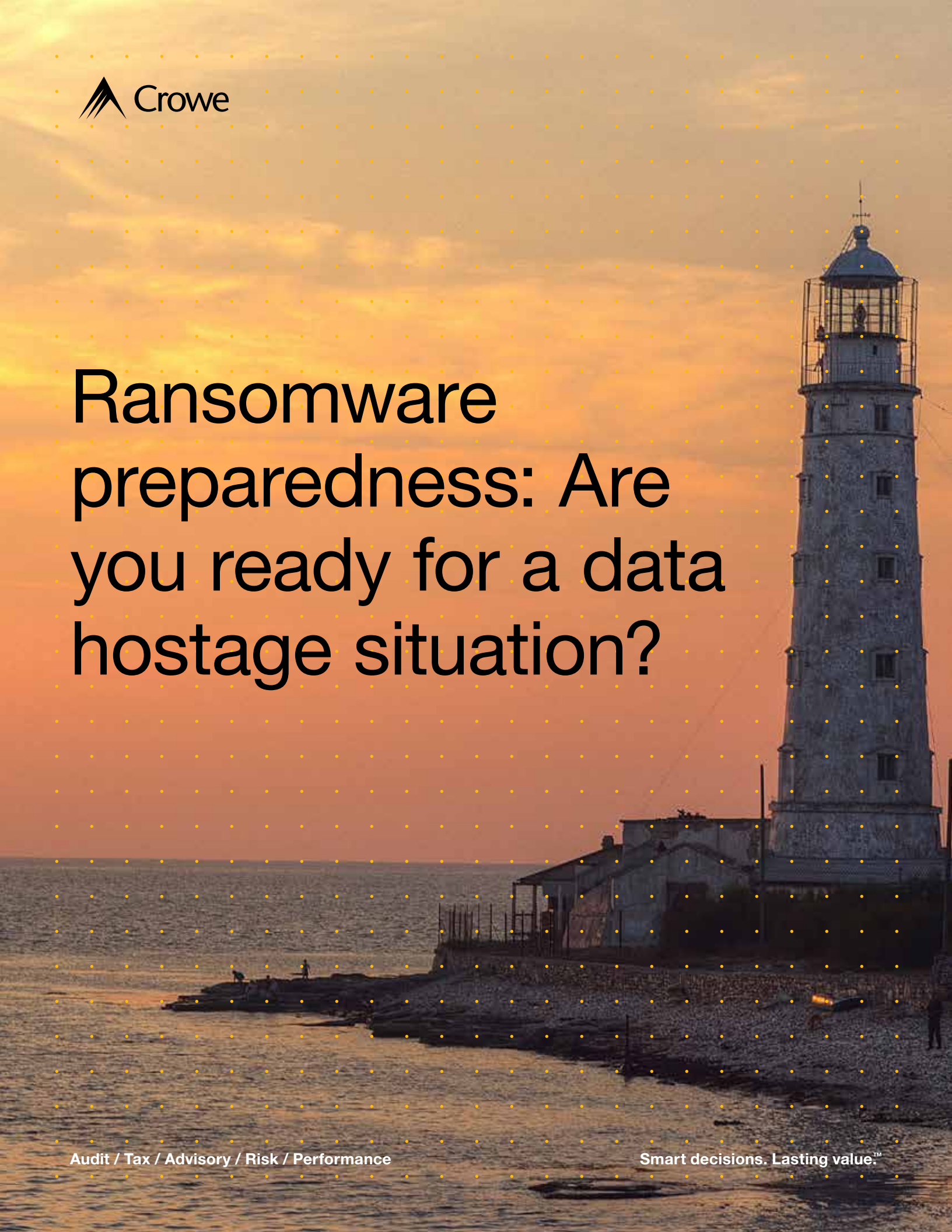
Crowe

Ransomware preparedness: Are you ready for a data hostage situation?



Audit / Tax / Advisory / Risk / Performance

Smart decisions. Lasting value.℠

Ransomware, a type of malicious software, is the most recent technique used to turn compromised computers into cash for criminals. The software holds data hostage while the attacker demands that victims pay a ransom to regain control of their data. This tactic is on the rise.

Although the sale of a credit card number, health record, or banking website password may fetch only a few dollars on the black market, a compromised machine that has been fully encrypted can be worth hundreds if not thousands of dollars. For larger organizations, the amount demanded as ransom is in the tens or hundreds of thousands of dollars. According to the FBI,[1] from April 2014 to June 2015, a single strain of ransomware was responsible for more than $18 million in losses across almost 1,000 instances.

What are the risks?

Ransomware, designed to prevent rightful owners from accessing their files, is a threat to both companies and individuals. Victims, in a last-ditch effort to recover precious data, send money to an anonymous entity in return for a decryption program. Although some victims pay and recover their data, others – regardless of whether they pay – have sensitive corporate data permanently locked, often forcing the organization to revert to data backups. School districts, hospitals, banks, and government organizations have had operations grind to a halt as network and systems engineers rush to contain and eradicate the threat from their systems.

How does infection occur?

The delivery mechanisms for ransomware are similar to other types of viruses found on the Internet: an email attachment or link opened by an unsuspecting user, an advertisement loaded into a commonly browsed and otherwise safe website, or a malicious office productivity tool downloaded and installed by a user. Once the ransomware program accesses the system, it calls out to a server on the Internet to obtain the encryption key to use. Then, the malicious code begins to identify and encrypt documents, spreadsheets, presentations, emails, photos, and videos not only on the local hard drive but on attached USB devices and network shared drives. In a corporate environment where network shared drives are often accessible by everyone in the same department or company, huge data stores can be threatened by a single infection initiated by an end user.

Are there options besides paying?

Some earlier variants of ransomware were known to have bugs allowing security researchers to reverse engineer the software by writing a custom decryption program. This option is by far the exception because many ransomware applications have been patched. Most analyzed ransomware samples use industry-standard algorithms and key lengths to lock files with the same strength of encryption used to protect e-commerce transactions and classified national security information. The chance of forcing a break in the encryption is near zero.

Strong data backup processes and procedures are a good defense but not something organizations can implement after an infection.

Ransomware preparedness assessment by Crowe

To determine the ability to withstand such an attack, Crowe takes a systematic approach to testing each phase of the infection. Because of the complexity of computer networks, systems, and security mechanisms, understanding which controls are in place, how effective they are, and where the risk lies is important in developing mitigating strategies for ransomware. Areas of review include:

- **Email filtering**. Email is a must-have in today's corporate world. Simply providing email introduces some level of risk to the environment as it allows attackers to directly reach internal employees with access to sensitive information. Crowe tests various email formats and evasion techniques in an attempt to bypass security controls and determine what is allowed to be delivered to your end users.
- **Social engineering**. The end user is often referred to as one of the weakest and most unpredictable links in the security chain. Prompting someone on the inside to introduce malicious code into the environment still proves to be a successful attack vector for criminals. Crowe emulates this behavior with tools and tactics similar to real-world attacks, allowing clients to gauge the effectiveness of their employee security awareness program.
- **Endpoint protection**. Once malicious code has entered the environment, many security suites are designed to engage and neutralize the threat. Signature-, behavioral-, and anomaly-based malware detection strategies can all be effective at the endpoint but have their weaknesses and can be evaded. Different malware samples and behavior can be replicated by Crowe to test the blind spots of these solutions.
- **Propagation**. Limiting the movement of malicious code is significant to minimizing impact. Preventing malicious code from obtaining administrative privileges or moving through the network shortens response timelines, limits exposure, and ultimately keeps down costs. Crowe identifies these avenues for granting administrative privileges and helps clients develop corresponding alerting or blocking mechanisms.
- **Data backup procedures**. Examination of backup procedures and their frequency can help confirm that critical information is accessible. Failure to properly back up data or test controls can result in few options after a ransomware attack. With a systematic approach, Crowe examines these processes and procedures to identify the strength of the implemented controls.
- **Data exfiltration**. Organizations are often unaware of the vast ways in which data can leave their networks. Some organizations have implemented data loss prevention programs and tools to alert and restrict this data movement. Crowe can test the following vectors associated with data exfiltration:
  - Outbound email filtering
  - Web traffic proxy and filtering
  - Firewall traffic analysis
  - Covert network channels
  - Egress detective controls
- **Incident response**. A properly developed, implemented, and tested incident response program can make the difference between a large-scale infection and a single compromised host. Acting quickly and decisively from a technical, managerial, and public affairs standpoint can vastly limit the impact from such an attack. Crowe has experience helping clients develop and test incident response plans and programs. Additionally, trained and experienced personnel are available to augment staff in investigations, forensics acquisition, and data preservation.

Ransomware is a growing threat affecting individuals, small businesses, and large corporations. Although a strong response to an attack is critical to limit the impact, identifying the gaps, preparing your network, and testing controls will reduce the risk and exposure to one of today's fastest-growing cybercrimes.

Contact information

For more information, please contact:

Kiel Murray
+1 214 777 5241
kiel.murray@crowe.com

Christopher Wilkinson, Principal
+1 219 308 8980
christopher.wilkinson@crowe.com

[1] "Criminals continue to defraud and extort funds from victims using cryptoWall ransomware schemes," FBI, June 23, 2015, https://www.ic3.gov/media/2015/150623.aspx

About Crowe

"Crowe" is the brand name under which the member firms of Crowe Global operate and provide professional services, and those firms together form the Crowe Global network of independent audit, tax, and consulting firms. Crowe may be used to refer to individual firms, to several such firms, or to all firms within the Crowe Global network. The Crowe Horwath Global Risk Consulting entities, Crowe Healthcare Risk Consulting LLC, and our affiliate in Grand Cayman are subsidiaries of Crowe LLP. Crowe LLP is an Indiana limited liability partnership and the U.S member firm of Crowe Global. Services to clients are provided by the individual member firms of Crowe Global, but Crowe Global itself is a Swiss entity that does not provide services to clients. Each member firm is a separate legal entity responsible only for its own acts and omissions and not those of any other Crowe Global network firm or other party. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global.

www.crowe.com

RISK-17005-009A