

September 24, 2019

# Ransomware Still a Growing Problem for Organizations of All Sizes

CYBERSECURITY

BY SEAN THOMAS

SHARE WITH A COLLEAGUE



DOWNLOAD PDF



While the concept of malware-based extortion has remained relatively unchanged since the first documented occurrence in 1989, attackers have spent the past 30 years refining their techniques and manipulating new technologies to build ransomware into a multibillion dollar industry.

Tactics have evolved from the early days when physical floppy disks were mailed out containing the “AIDS Trojan” with the hope that unsuspecting targets would load the malware onto their PCs. Even just a few years ago, ransomware such as “WannaCry” and “CryptoLocker” was spread via widespread phishing campaigns that were generally not tailored to specifically targeted individuals or groups. But today, ransomware is increasingly deployed as a secondary attack after the bad actor has already gained a solid foothold in the organization’s internal network.

Weekly, we are seeing new headlines revealing the latest victims of ransomware: state and local government offices, educational institutions, healthcare providers, and small and medium-sized businesses. Often the attacks are tailored and use advanced methods that disable the organizations’ critical resources and demand ransom payments large enough to cripple operations. Public utilities have seen billing disrupted for months, police departments have been forced to revert to paper recordkeeping, and local governments have been reduced to issuing official statements about the outages via handwritten memos.

This past August, 22 cities in Texas were attacked simultaneously and held ransom for \$2.5 million as the result of the breach of a shared third-party. Earlier this summer, Lake City, Florida paid a ransom of almost half a million dollars rather than attempt to recover its systems from backups. Cities that have chosen not to pay ransoms, such as Atlanta and Baltimore, have faced recovery costs of several million dollars even with reliable system backups.

An event of that magnitude can quickly threaten the existence of a small or medium-sized business, but the process of preparing to face the threat of ransomware does not need to be overwhelming. Managing this risk requires focusing on three main activities:

## 1. Prevent

Standard cyber-hygiene such as anti-virus and patch management still applies, but organizations should also be considering how to limit damage if an endpoint, or – increasingly – a service provider, is compromised. An email protection platform like **Mimecast®** adds an additional layer of defense from the most common means of compromise: phishing.

## 2. Detect

Next-generation endpoint protection platforms such as **Carbon Black®** help detect suspicious activity, and when possible, remediate the issue before it can propagate throughout the network. Organizations of all sizes should be employing properly tuned automation platforms to sift through system event data and flag potential security concerns.

## 3. Respond

Simply performing regular system backups does not constitute an adequate approach to disaster recovery. Organizations should ensure that appropriate plans are in place to manage cyber incidents and that these plans, as well as the organization's data backups, are regularly tested.

### How can Schneider Downs help?

The Schneider Downs cybersecurity practice consists of experts in multiple technical domains. Schneider Downs is an authorized reseller of both **Mimecast®** and **Carbon Black®**, and offers comprehensive [digital forensics and incident response](#) services. For more information on our available services and software, please contact us at [cybersecurityteam@schneiderdowns.com](mailto:cybersecurityteam@schneiderdowns.com).

Our whitepaper outlining some of top preventative measures organizations overlook is available here: <https://schneiderdowns.com/10-things-companies-wish-they-did-before-a-breach>.

SHARE



## You've heard our thoughts... We'd like to hear yours

The Schneider Downs Our Thoughts On blog exists to create a dialogue on issues that are important to organizations and individuals. While we enjoy sharing our ideas and insights, we're especially interested in what you may have to say. If you have a question or a comment about this article – or any article from the Our Thoughts On blog – we hope you'll share it with us. After all, a dialogue is an exchange of ideas, and we'd like to hear from you. Email us at [contactSD@schneiderdowns.com](mailto:contactSD@schneiderdowns.com).

Material discussed is meant for informational purposes only, and it is not to be construed as investment, tax, or legal advice. Please note that individual situations can vary. Therefore, this information should be relied upon when coordinated with individual professional advice.

© 2019 Schneider Downs. All rights-reserved. All content on this site is property of Schneider Downs unless otherwise noted and should not be used without [written permission](#).



CYBERSECURITY BY MATTHEW DUNN

10.30.2019

## Questions to Ask Before Ransomware Hits Your Business

[READ MORE >](#)

Register to receive our weekly newsletter with our most recent columns and insights.

[SUBSCRIBE FOR UPDATES](#)

### MOST RECENT

#### Impact of Tax Reform on Accounting for Income Taxes – Changes in NOL

**TAX**  
BY [JAMES SAYRE](#) | 11.8.2019

The Tax Cuts and Jobs Act of 2017 (TCJA) impacted nearly every U.S. taxpayer both in personal income tax filings, and indirectly through the changes in ...

[READ MORE](#)

### MOST POPULAR

#### Tax Treatment of Deferred Revenue in a Taxable Stock Acquisition

**MERGERS AND ACQUISITIONS, TAX**  
BY [GARY SLIMAN](#) | 6.1.2016

The general rule under Internal Revenue Code §451 is that an item of income shall be included in gross income for the taxable year or receipt unless ...

[READ MORE](#)



Have a question? Ask us!

We'd love to hear from you. Drop us a note, and we'll respond to you as quickly as possible.

ASK US

## CONTACT US



### PITTSBURGH

One PPG Place, Suite 1700  
Pittsburgh, PA 15222

[contacts@schneiderdowns.com](mailto:contacts@schneiderdowns.com)  
p:412.261.3644 f:412.261.4876



### COLUMBUS

65 East State Street, Suite 2000  
Columbus, OH 43215

[contacts@schneiderdowns.com](mailto:contacts@schneiderdowns.com)



**WASHINGTON, D.C.**

1660 International Drive, Suite 600  
McLean, VA 22102

[contacts@schneiderdowns.com](mailto:contacts@schneiderdowns.com)

p:571.380.9003



**FOLLOW US**



**CLIENT PORTAL**



**SUBSCRIBE FOR UPDATES**

E-mail

SUBMIT





[PRIVACY POLICY](#)

[LEGAL INFORMATION](#)

[SITE MAP](#)

Schneider Downs is a Top 60 independent Certified Public Accounting (CPA) firm providing accounting, tax, audit and business advisory services to public and private companies, not-for-profit organizations and global companies. We also offer Internal Audit; Technology Consulting; Software Solutions; Personal Financial Services; Retirement Plan Solutions and Corporate Finance Services. Schneider Downs is the 13th largest accounting firm in the Mid-Atlantic region and serves individuals and companies in Pennsylvania (PA), Ohio (OH), West Virginia (WV), New York (NY), Maryland (MD), and additional states in the United States with offices in Pittsburgh, PA and Columbus, OH.

© 2019 Schneider Downs & Co., Inc. Maryland license number 35239