UT LAW CLE THE UNIVERSITY OF TEXAS SCHOOL OF LAW

PRESENTED AT

2018 School Law Conference

February 22-23, 2018
Austin, TX

Under Attack!
Minimizing the Risk and Mitigating the Impact of Cybercrime

Brett E. Leatherman
Mari McGowan

Brett E. Leatherman, CISSP, GISP, GSEC
Supervisory Special Agent
Federal Bureau of Investigation
Dallas Division

Mari McGowan
Director/Shareholder
Abernathy, Roeder, Boyd & Hullett, P.C.
1700 Redbud #300
McKinney, TX 75069
(214)-544-4000

UNDER ATTACK! MINIMIZING THE RISK AND MITIGATING THE IMPACT OF CYBERCRIME

TABLE OF CONTENTS

I. Introduction

In the fall of 2017, a Johnston, Iowa parent received an anonymous text message: "Your child still looks so innocent. Don't let your child go outside."[1] Time went on, and the messages became more threatening – and more specific.[2] The texts made mentioning the child by the correct name and school.[3] More and more parents received the anonymous messages, which continued to grow more graphic.[4] The group that claimed responsibility for the hacks posted the students' phone numbers and names online, encouraging predators to target them.[5] District officials shut down eight schools so law enforcement could conduct sweeps with bomb-sniffing canines.[6] Meanwhile, parents began receiving similar messages at districts in Texas and Montana. In Montana, the Columbia Falls School District received a seven-page ransom letter demanding $75,000 in Bitcoin in exchange for a promise to not release student data obtained from the district's computer system.[7] Several dozen schools closed for three days in response to the threats.[8]

Ultimately, a group named "Dark Overlord" took responsibility for the attacks.[9] The heavy-handed moniker almost induces laughter, but these attacks represent a serious threat to American colleges and school districts. Other such examples of recent cyber-attacks include the 2015 UCLA Medical System breach, where hackers gained access to the data of 4.5 million people.[10] At Ohio State University, a cyber-attack exposed the data of more than 760,000 individuals, and cost the school over $4 million to investigate and

---

[1] Moriah Balingit & Valerie Strauss, *Education Department warns of new hacker threat as 'Dark Overlord' claims credit for attacks on school districts*, WASHINGTON POST (Oct. 26, 2017), https://www.washingtonpost.com/news/answer-sheet/wp/2017/10/26/education-department-warns-of-new-hacker-threat-as-dark-overlord-claims-credit-for-attacks-on-school-districts/?utm_term=.a0613d3a387b.
[2] *Id*.
[3] *Id*.
[4] *Id*.
[5] *Id*.
[6] *Id*.
[7] *Id*.
[8] *Id*.
[9] *Id*.
[10] Jose Pagliery, *UCLA Health hacked, 4.5 million victims*, CNN (July 17, 2015, 6:47 PM), http://money.cnn.com/2015/07/17/technology/ucla-health-hack/index.html

remedy.[11] As colleges and school districts become increasingly dependent upon technology, the threat posed by cyber-attacks will likewise expand. What can colleges and school districts do to protect themselves from cyber-attacks and other forms of cybercrime? This paper examines some of the most common forms of cybercrime, and provides an overview of best practices for preventing and mitigating the damage caused by cyber-attacks.

II. Overview of Cybercrimes

A. Business E-mail Compromise & CEO Fraud

The Federal Bureau of Investigation's Internet Crime Complaint Center ("IC3") defines "business e-mail compromise", or BEC, as "a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds."[12] Put more simply, the criminals using business e-mail compromise rely on deception.[13] Victims commonly report using either wire transfer or checks as a payment method, and criminals will use the preferred method of their victim's normal business practices.[14] The FBI reports a 1,300% increase in identified exposed losses between January 2015 and June 2016.[15]

Entities perpetuating business e-mail compromise scams attempt to identify the individuals and protocols necessary to perform wire transfers within a particular business or organization's operating environment.[16] Victims may receive "phishing" e-mails requesting additional details regarding the targeted organization or individual, such as

[11] Tamar Lewin, *Ohio State Says Hackers Breached Data on 760,000*, NEW YORK TIMES (Dec. 16, 2010), http://www.nytimes.com/2010/12/17/education/17colleges.html.
[12] *Business E-mail Compromise: The 3.1 Billion Dollar Scam*, INTERNET CRIME COMPLAINT Center (June 14, 2016), https://www.ic3.gov/media/2016/160614.aspx.
[13] *Id*.
[14] *Id*.
[15] *Id*.
[16] *Id*.

Title search: Under Attack! Minimizing the Risk and Mitigating the Impact of Cybercrime

Also available as part of the eCourse
Cybersecurity Planning for Schools: Minimizing the Risk and Mitigating the Impact

First appeared as part of the conference materials for the
33rd Annual School Law Conference session
"Under Attack! Minimizing the Risk and Mitigating the Impact of Cybercrime "