ALFA International
The Global Legal Network
Celebrating 40 Years

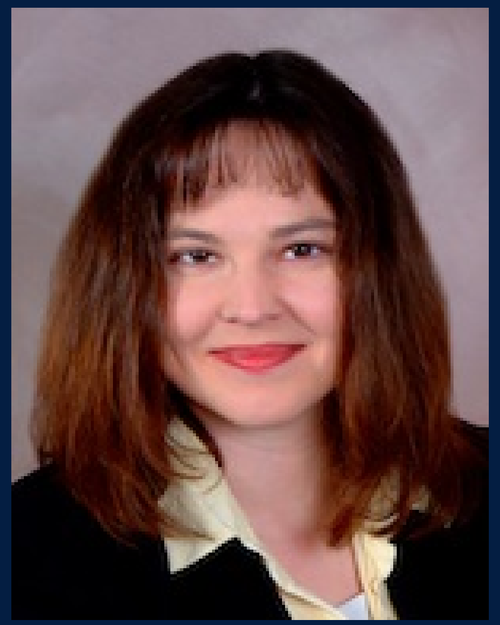
PROTECTING YOUR FIRM'S DATA WHILE PERMITTING REMOTE WORK: TECHNOLOGICAL COMPETENCE AND ETHICAL REQUIREMENTS

MAY 27, 2020

PRESENTERS

Devin Chwastyk
McNees Wallace & Nurick
Harrisburg, PA
E: dchwastyk@mcneeslaw.com
T: 717.237.5482

A.J. Singleton
Stoll Keenon Ogden, PLLC
Lexington, KY
E: aj.singleton@skofirm.com
T: 859.231.3692



Leslie Whitten
Young Clement Rivers LLP
Charleston, SC
E: lwhitten@ycrlaw.com
T: 843.724.6642

ALFA International
The Global Legal Network
Celebrating 40 Years

HEIGHTENED CLIENT EXPECTATIONS …

More Than 100 Law Firms Have Reported Data Breaches. And the Problem Is Getting Worse

A Law.com investigation finds that law firms are falling victim to data breaches at an alarming rate, exposing sensitive client and attorney information. These incidents—most unpublicized before now—may just be the tip of the iceberg.

By **Christine Simmons**, **Xiumei Dong** and **Ben Hancock** | October 15, 2019 at 01:10 PM

As Hackers Get Smarter, Can Law Firms Keep Up?

"It's not the hardware you worry about. It's the mistake that someone makes that inadvertently gives a bad actor access," said one law firm cybersecurity partner.

By **Christine Simmons** and **Xiumei Dong** | October 28, 2019 at 05:30 AM

Increasing Client Requirements: Securing Law Firms for the 21st Century

Gone are the days of "basic security." What used to be optional is now standard: two factor authentication, complex passwords, clean desk policies, data encryption at rest and in transit, mobile device management and up-to-the-minute patching. Clients expect these items to already be in place and are further expanding their expectations.

By **Debra Gray** | October 29, 2019 at 03:48 PM

ALFA International
The Global Legal Network
Celebrating 40 Years

… AND EMERGING THREATS!

Warning to law firms: a ransomware group is stealing data and posting it online

EMSISOFT MALWARE LAB · FEBRUARY 3, 2020 · 4 MIN READ

Ransomware Attacks Hit Three Law Firms in Last 24 Hours

By Bob Ambrogi on February 1, 2020

Maze Ransomware Attack Has Hit Small Law Firms in 3 States

The ransomware attack on three small South Dakota firms the hacker group touted online late last month follows previously announced hacks of firms in Texas and Oregon.

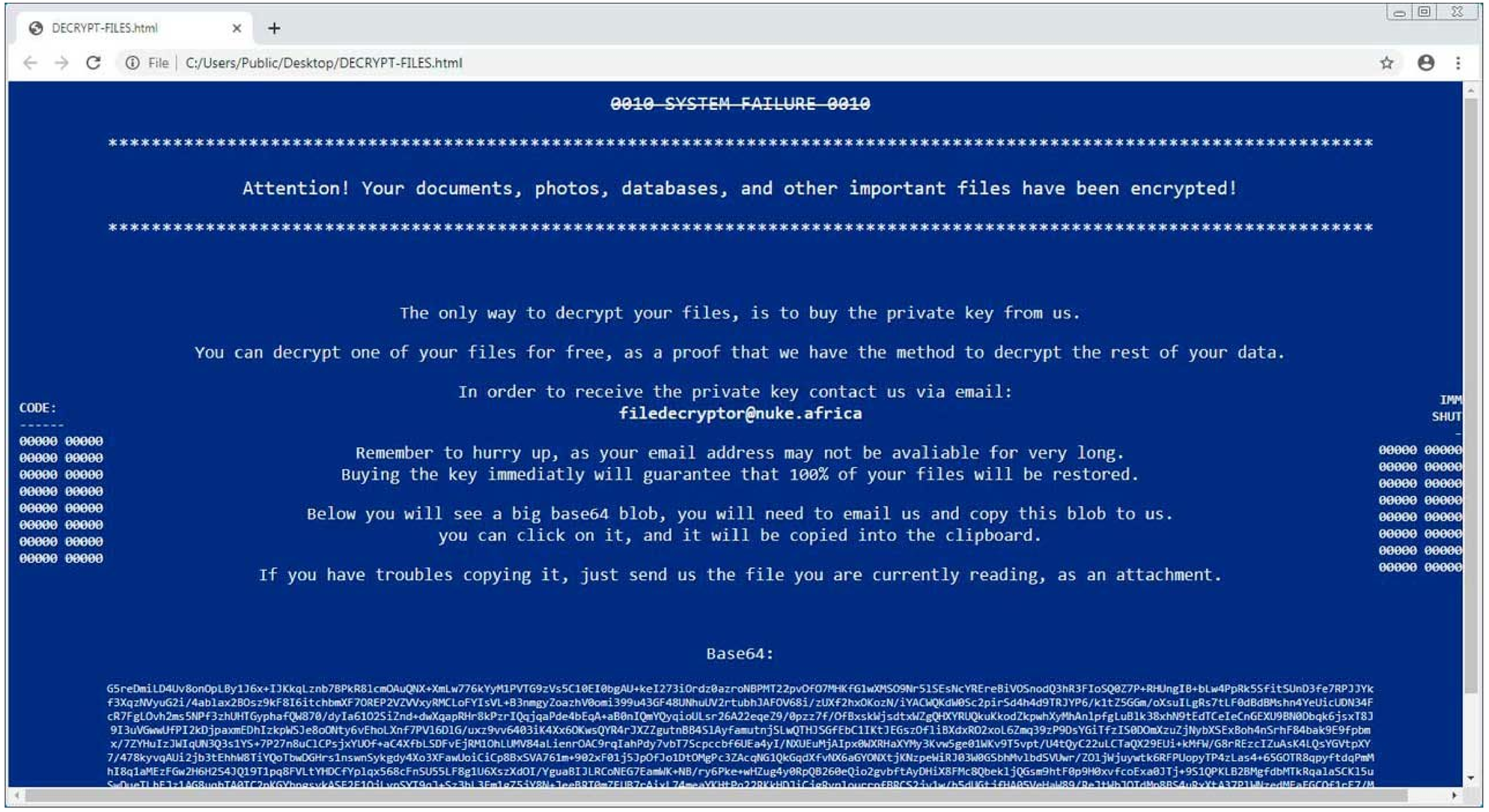
By **Patrick Smith** | February 04, 2020 at 07:24 PM

ALFA International
The Global Legal Network
Celebrating 40 Years

THE SCENARIO …

ALFA International
The Global Legal Network
Celebrating 40 Years

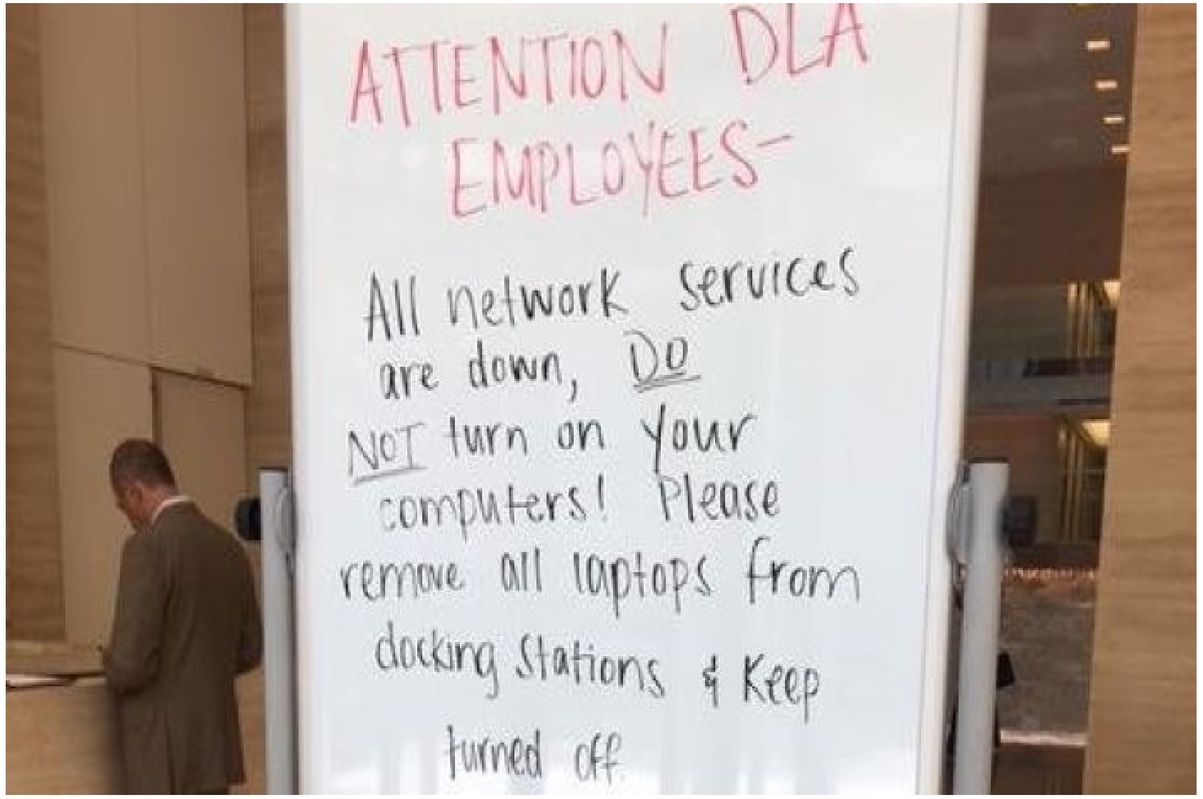
THE SCENARIO …



ALFA International
The Global Legal Network
Celebrating 40 Years

THE SCENARIO

- Your law firm's systems have been infected with the Maze ransomware variant
- No access to your computer systems
- Files contain both personally-identifiable information and confidential client information

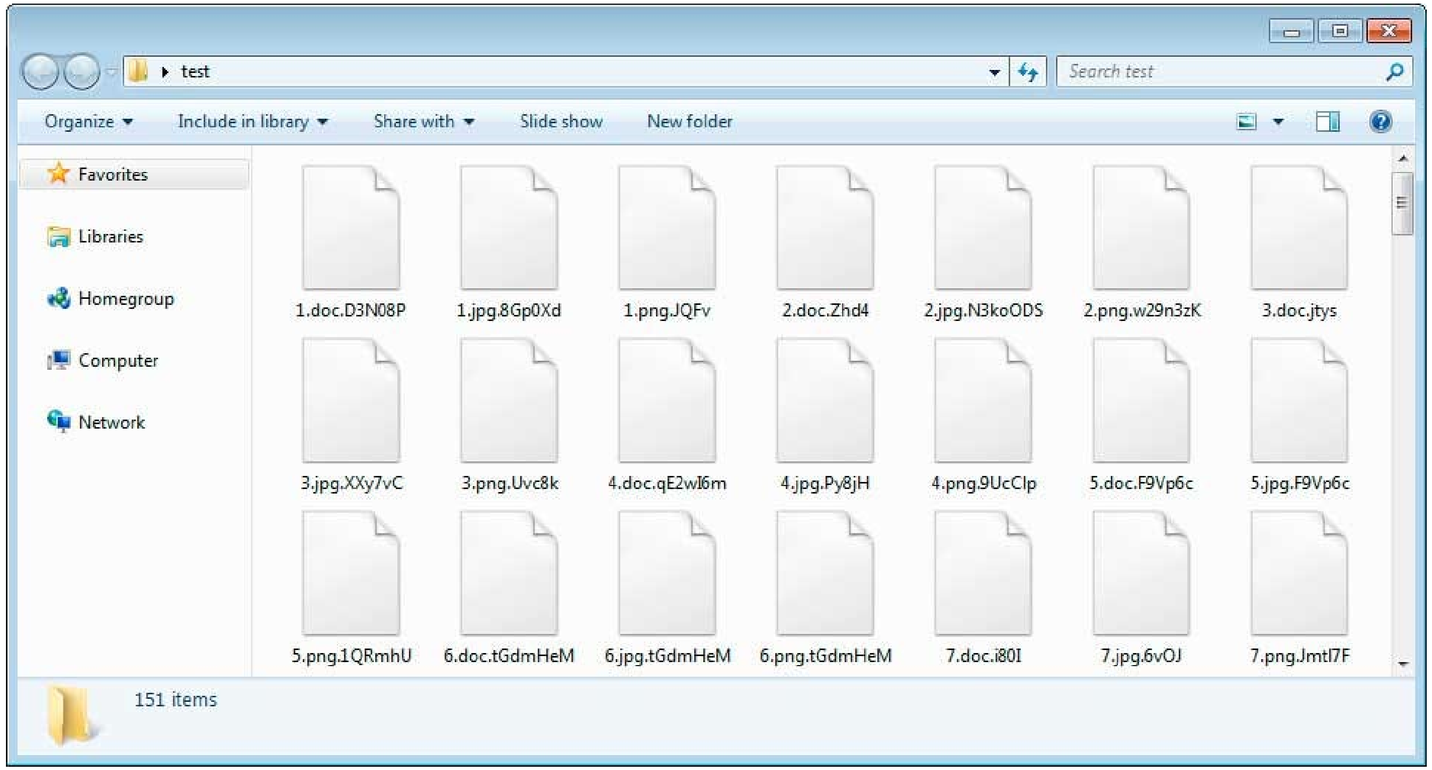


ALFA International
The Global Legal Network
Celebrating 40 Years

THE SCENARIO

- Hackers are demanding a ransom of 200 bitcoin (approximately $1.6 million)

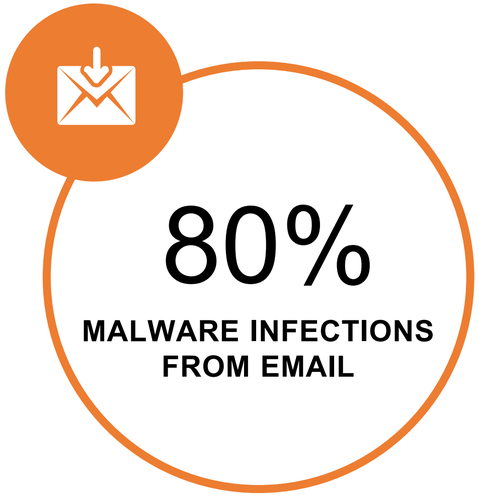
- Hackers threaten to begin posting files to the Dark Web if the ransom is not paid in 4 days



ALFA International
The Global Legal Network
Celebrating 40 Years

HOW DID THIS HAPPEN?

- Phishing
  - Credential Theft
  - Malicious links/attachments
- Malware
  - Viruses
  - Worms
  - Trojans
- Exploitable Vulnerabilities



ALFA International
The Global Legal Network
Celebrating 40 Years

WHAT HAPPENS NEXT?

- Does your firm have an incident response plan?
  - Who is your incident response team?
- Would you contact law enforcement?
- How soon do you involve internal/outside counsel?
  - Who is responsible for hiring the external forensic investigator?
- Do you have cyber liability insurance?
  - Are your malpractice premiums paid up?

WHAT HAPPENS NEXT?

- Would your firm pay the ransom?
- What factors would you consider in your decision regarding paying the ransom?
  - How long would it take to recover from backups?
  - How long would it take to recover if the decryption key is purchased?
- Does your firm have a bitcoin account? And $7 million in bitcoin?
- Does your insurance cover payment of a ransom?

ALFA International
The Global Legal Network
Celebrating 40 Years

WHAT HAPPENS NEXT?

- When do you consider informing your clients?
  - Do you have enough information to determine whether there is a reportable breach?
  - Does it matter whether the infected files contain personally-identifiable vs. client confidential information?
- Does it matter whether the hackers have begun releasing the files on the Dark Web?
  - Media attention?

ALFA International
The Global Legal Network
Celebrating 40 Years

THE CLIENT'S PERSPECTIVE

- Engagement Agreements/Data Security Addenda
- Vendor Data Security Questionnaires
- Security Audits/Assessments

THE FIRM'S ETHICAL, LEGAL, AND CONTRACTUAL OBLIGATIONS

- Sources of Obligations:
  - Rules of Professional Conduct
  - State privacy laws
  - Engagement letters/Contractual Obligations

THE FIRM'S ETHICAL OBLIGATIONS

- Rules of Professional Conduct
  - Rule 1.1 Competency
  - Rule 1.6 Confidentiality
  - Rule 1.15 Duty to safeguard client property
  - Rule 5 Duty to supervise
  - Rule 1.9 Duties to former clients

THE FIRM'S ETHICAL OBLIGATIONS

- ABA Formal Opinion 477 (2017)
  - What is "reasonable security" for law firms?

POP UP QUESTION

- What authorities impose cybersecurity requirements on attorneys and law firms?
  A. The Rules of Professional Conduct
  B. State bar ethical opinions
  C. Client engagement letters and data security agreements
  D. All of the above

“REASONABLE SECURITY” TO PROTECT LAW FIRM DATA

- A written information security policy;
- Regular training of attorneys and staff;
- Record retention policies, data classification, and access controls;
- Incident response plan and war-gaming;
- Third-party security audits, risk assessments, and penetration tests;
- VPN’s for remote access;

- Data loss prevention: restrictions on data transfers and use of removable media;
- Physical access controls;
- Vendor assessment and agreements; and,
- Cyber liability insurance, in addition to malpractice insurance.

“REASONABLE SECURITY” TO PROTECT LAW FIRM DATA

- Wi-Fi network, modem, and router passwords
- Connect to office systems through secure connection (VPN/RDC)
- Use dedicated work computers; refrain from use of social media or personal email accounts
- Disconnect/mute listening devices (Alexa, Echo)
- Secure videoconference solutions (Zoom, GoToMeeting)
- Conduct sensitive conversations outside hearing of family members
- Be alert for COVID-related phishing emails and spoofs of emails from clients and co-workers

THE FIRM'S ETHICAL OBLIGATIONS

- ABA Formal Opinion 483 (2018)
  - When must lawyers notify clients of a data security incident?

STATE PRIVACY LAWS

- Breach notification laws
- California Consumer Privacy Act

QUESTIONS?

ALFA International
The Global Legal Network
Celebrating 40 Years

THANK YOU! IF YOU HAVE ANY QUESTIONS, PLEASE CONTACT ONE OF THE PRESENTERS

Devin Chwastyk
McNees Wallace & Nurick
Harrisburg, PA
E: dchwastyk@mcneeslaw.com
T: 717.237.5482

A.J. Singleton
Stoll Keenon Ogden, PLLC
Lexington, KY
E: aj.singleton@skofirm.com
T: 859.231.3692

Leslie Whitten
Young Clement Rivers LLP
Charleston, SC
E: lwhitten@ycrlaw.com
T: 843.724.6642

ALFA International
The Global Legal Network
Celebrating 40 Years