EDUCATIONAL TECHNOLOGY AND DATA SECURITY

2017 ACBO SPRING CONFERENCE

Resort at Squaw Creek, Lake Tahoe

May 22, 2017

Presented by:
Lisa R. Allred, Partner

aalrr
Atkinson, Andelson
Loya, Ruud & Romo
A Professional Law Corporation

Introduction

1. Malware/Ransomware
2. Data Security Legal Issues
3. Cloud Computing Issues

What Is It?

YOUR COMPUTER HAS BEEN LOCKED!

- *Malware*
  - Software that is specifically designed to disrupt, damage, or gain authorized access to a computer system.

- *Ransomware*
  - A form of malware that targets both human and technical weaknesses in organizations and individual networks in an effort to deny the availability of critical data and/or systems.

(See oxforddictionaries.com)

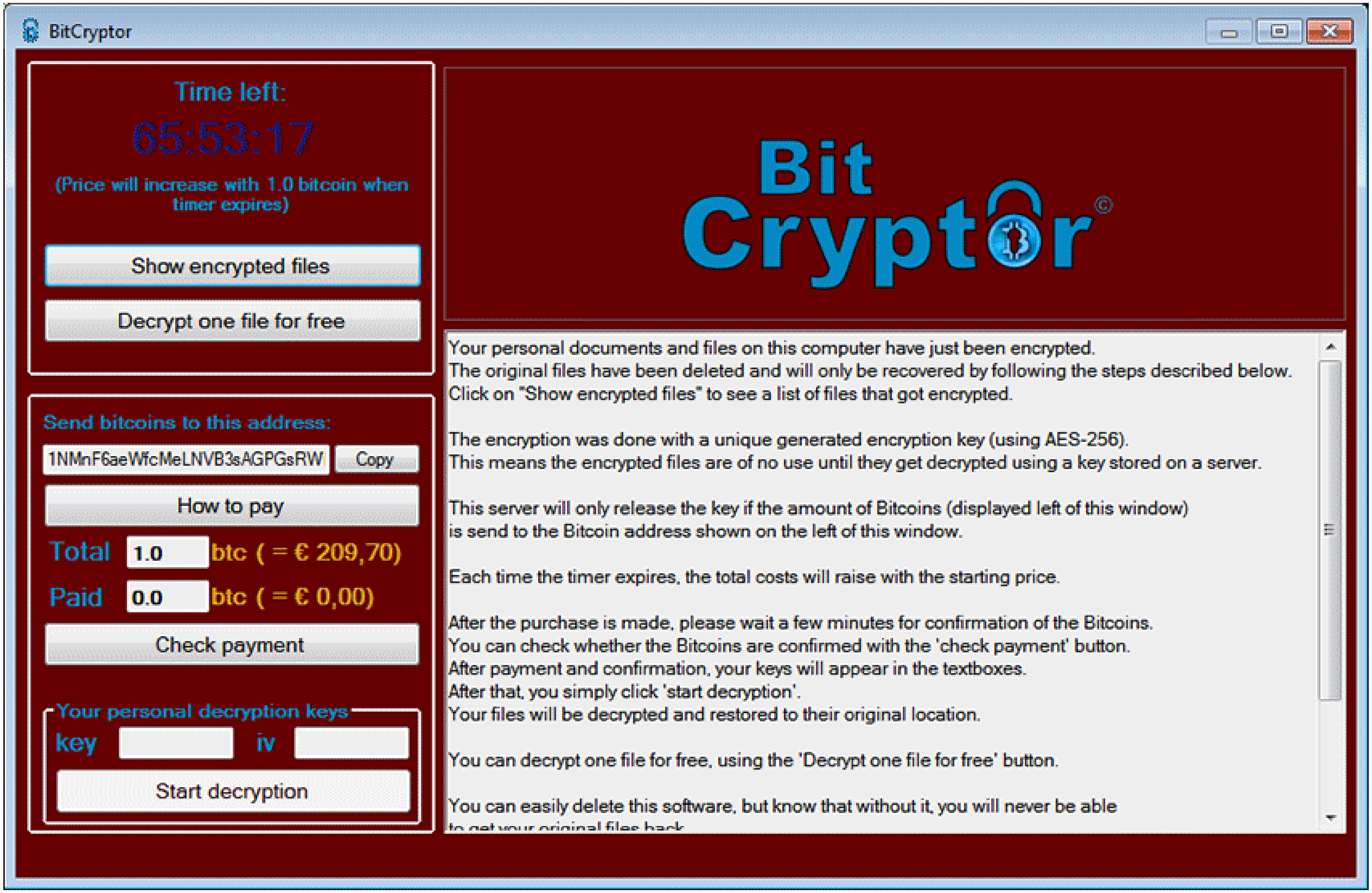
More On Ransomware

- How is a ransomware attack carried out?
  - Ransomware is frequently delivered through spear phishing emails to end users, resulting in the rapid encryption of sensitive files on a computer network.
  - Can also take the form of pop-up ads, or hyperlinks.

- In 2015, the Internet Crime Complaint Center (IC3) received 2,453 complaints identified as Ransomware with losses of over $1.6 million.
  - California: 271 Ransomware attacks costing $ 265,542

-See IC3 Report (2015), available at https://pdf.ic3.gov/2015_IC3Report.pdf.

How Do You Know?



Time left:

65:53:17

(Price will increase with 1.0 bitcoin when timer expires)

Send bitcoins to this address:

1NMnF6aeWfcMeLNVB3sAGPGsRW

Total 1.0 btc (= € 209,70)

Paid 0.0 btc (= € 0,00)

Your personal decryption keys

key iv

Your personal documents and files on this computer have just been encrypted.
The original files have been deleted and will only be recovered by following the steps described below.
Click on "Show encrypted files" to see a list of files that got encrypted.

The encryption was done with a unique generated encryption key (using AES-256).
This means the encrypted files are of no use until they get decrypted using a key stored on a server.

This server will only release the key if the amount of Bitcoins (displayed left of this window)
is send to the Bitcoin address shown on the left of this window.

Each time the timer expires, the total costs will raise with the starting price.

After the purchase is made, please wait a few minutes for confirmation of the Bitcoins.
You can check whether the Bitcoins are confirmed with the 'check payment' button.
After payment and confirmation, your keys will appear in the textboxes.
After that, you simply click 'start decryption'.
Your files will be decrypted and restored to their original location.

You can decrypt one file for free, using the 'Decrypt one file for free' button.

You can easily delete this software, but know that without it, you will never be able
to get your original files back

Response: To Pay Or Not to Pay?

- **What's it worth to not have access?**
  - Practical and financial considerations

- **The FBI does not support paying a ransom**
  - Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom.
  - Paying a ransom emboldens the adversary to target other organizations for profit, and provides for a lucrative environment for other criminals to become involved.

See FBI Brochure on ransomware available at: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-ceos.pdf/view

New law pertaining to data breaches:

AB 2828 (amending Civ. Code § 1798.29)

- Jan. 1, 2017: Closes the "encryption loophole," by requiring written notification of a data breach when **(1)** there is unauthorized acquisition of both encrypted PII and the encryption key or security credential; and **(2)** the agency has a reasonable belief that the PII will therefore be readable or usable.
- Previously, the data breach law was amended to define "encrypted," expand the definition of personal information, and update the requirements for a security breach notification letter. (Model Form at Civ. Code § 1798.82.)
- If breach notification is to more than 500 California residents (single breach), submit a single sample copy of that security breach notification to the Attorney General. https://oag.ca.gov/ecrime/databreach/report-a-breach
- If law enforcement is involved, notification "promptly" after law enforcement determines notice will not compromise investigation.

Ransomware Legal Update

- SB 1137, signed into law in Sept. 2016, clarified that deploying ransomware into a computer or system is a form of felony extortion (but…offshore criminals?).
- Law enforcement agencies advise that the criminals not receive payment.
- In many instances, the decryption key provided after payment does not work.

Avoiding Ransomware Issues

- Back up data regularly. Security consultants advise that backup services not be assigned a drive letter to avoid mapping/locating and cutting off access to that backup data

- Keep software up to date to prevent vulnerabilities, educate users on “fake” software updates, and educate system users to avoid introduction of malware

- Ensure remote access is secure, and use secure WiFi

Data Breaches – Current and Future

- Predicted that with implementation of chip-enabled payment cards, criminals will focus on SSN theft

- AB 2097 (2016) amended Ed Code 49076.7(b) to prohibit collecting or soliciting SSNs or last 4 digits from students/parents unless required by law
- Types of Breach:
  - Malware, hacking (54%)
  - Physical breaches/device theft (17%)
  - Human error (misdelivery of email, inadvertent public Internet posting) (17%)

Third Party Applications and Systems

Legal Issues

- Contracts
- Record Retention
- California Public Records Act
- Ownership
- Intellectual Property Rights and Obligations
- Data Security
- Data Mining

Data Mining

- Data mining is the practice of automatically searching large stores of data to discover patterns and trends that go beyond simple analysis.
- Data mining uses sophisticated mathematical algorithms to segment the data and evaluate the probability of future events.
- Data mining is also known as Knowledge Discovery in Data (KDD)

Data & Disclosure Laws That Impact Educational Institutions

- Federal Laws
  - Family Educational Rights and Privacy Act (FERPA) for Educational Institutions
    - Student Records
  - Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)
    - Medical Records
  - Gramm-Leach-Bliley Act
    - Financial Records
  - Payment Card Industry Data Security Standards (PCI-DSS)
    - Credit Cards/Payment Cards

Vendor Agreements

"No One Ever Asked for that Before"

- Institution must identify the legal and practical ramifications associated with the technology project.
  - Institutions remain liable for their data and operations even though a vendor is involved.
  - If you have to comply with laws, so does the vendor!
  - Responsibilities and risks must be allocated between the vendor and the institution.
- Some vendors may not be aware of the many legal parameters binding educational institutions.
- Both parties must be educated about the legal issues.
- Vendor must be willing to accept responsibilities in the technology agreement.
  - Complying with litigation holds, discovery requests, and/or subpoenas
  - Records retention laws and policies (e.g. Requests made under the CPRA)
  - Insurance? (Cyber risks must be identified.)

Other Technology Contract Terms

- **Ownership of Data**
  - Confirm language in agreements does not transfer to vendor any rights in institution's data.
  - No data mining or use of your institution's information for vendor's business or marketing purposes.
  - Education Code section 49073.1 requires certain contracts between local educational agencies and third parties to include specified provisions about the security, use, ownership, and control of pupil records.

- **Termination of Agreement**
  - Who owns the data?
  - What and how will institutional data be returned (will it be in a usable format?)
  - Implementation of termination: What is your plan?

Vendors Want You to Indemnity Them for Their Failures

- Sample Vendor Clause:
  - YOU AGREE TO HOLD HARMLESS, INDEMNIFY AND, AT VENDOR’S REQUEST, DEFEND VENDOR, ITS AFFILIATES AND THEIR RESPECTIVE OFFICERS, DIRECTORS, AGENTS AND EMPLOYEES (COLLECTIVELY, “VENDOR PARTIES”) FROM AND AGAINST ANY AND ALL CLAIMS (INCLUDING LIABILITIES, DAMAGES, LOSSES, COSTS AND EXPENSES AND REASONABLE ATTORNEYS' FEES) TO THE EXTENT ARISING OUT OF ANY ACTION OR PROCEEDING BROUGHT BY A THIRD PARTY AGAINST ANY ONE OR MORE OF THE VENDOR PARTIES RELATED TO THIS AGREEMENT.

Vendors Want You To Indemnity Them for Their Failures

- **TRANSLATION**
  - YOU ARE RESPONSIBLE FOR VENDOR'S FAILURES THAT CAUSE INJURY TO OTHERS.

- **SOLUTION**
  - Require Vendor to indemnify your institution for data breach, breach of agreement, general negligence and IP infringement.
  - Make sure clause is not undermined by limitation of liability clause.

Other Issues

- Possible negligence claims
- Discipline of students and employees
- Public Relations

Education

- Implement an awareness and training program

- Educate them on internet security
  - Don’t open attachments from unknown sources
  - Beware of attachments with .exe on them
  - Beware of phishing emails
  - Highlight vulnerabilities of peer-to-peer file sharing

- Make sure important information gets backed up

- Use the same precautions on your mobile phone as you would your computer

- Teach good security habits

Preparations:
Response Plan and Best Practices

Preparing for an attack/breach

1. Have a written plan
2. Identify your response team
3. Consider insurance options ahead of time
4. Conduct an inventory

Responding to an Attack or Breach:

1. Investigate immediately
2. Notify and consult with counsel
3. Notify law enforcement
4. Consider consultants (IT, PR, Forensics, Security)

Responding to an Attack or Breach:

5 Is notification required and, if so, to whom?

6 Have clear communication strategies

7 Determine insurance coverage and tender as appropriate

8 Learn from the incident

Conclusion & Takeaway Message

- ***Educate*** employees and students of the risks
- ***Remind*** employees and students that IT is there to help
- ***Start*** planning a response protocol

Thank You

For questions or comments, please contact:

{ Lisa R. Allred
(916) 923-1200
lallred@aalrr.com }

aalrr

Atkinson, Andelson
Loya, Ruud & Romo
A Professional Law Corporation

Disclaimer

This AALRR presentation is intended for informational purposes only and should not be relied upon in reaching a conclusion in a particular area of law. Applicability of the legal principles discussed may differ substantially in individual situations. Receipt of this or any other AALRR presentation/publication does not create an attorney-client relationship. The Firm is not responsible for inadvertent errors that may occur in the publishing process.