About the Presenter

Jeffrey Kline

- 27 years of information technology and information security experience
- Master of Science in Information Systems from Dakota State University
- Technology and Management Consulting with RSM
- Located in Sioux Falls, South Dakota
  - Rapid Assessment®
  - Data Storage SME
  - Virtual Desktop Infrastructure
  - Microsoft Windows Networking
  - Virtualization Platforms
INTRODUCTION TO CYBERCRIME
Cybercrime

Cybercrime is any type of criminal activity that involves the use of a computer or other cyber device.
- Computers used as the tool
- Computers used as the target

Long History of Cybercrime

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1971</td>
<td>John Draper uses toy whistle from Cap’n Crunch cereal box to make free phone calls</td>
</tr>
<tr>
<td>1973</td>
<td>Teller at New York Dime Savings Bank uses computer to funnel $1.5 million into his personal bank account</td>
</tr>
<tr>
<td>1981</td>
<td>First convicted felon of a cybercrime – “Captain Zap” who broke into AT&amp;T computers</td>
</tr>
<tr>
<td>1983</td>
<td>UCLA student used a PC to break into the Defense Department’s international communication system</td>
</tr>
<tr>
<td>1984</td>
<td>Counterfeit Access Device and Computer Fraud and Abuse Act was passed</td>
</tr>
</tbody>
</table>
### Long History of Cybercrime (continued)

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1994</td>
<td>Russian hackers steal $10 million from Citibank and distribute the money to bank accounts around the world</td>
</tr>
<tr>
<td>1995</td>
<td>European Trekies / hackers compromised Newscorp / SKY-TV to allow illegal access to Star Trek re-runs in Germany</td>
</tr>
<tr>
<td>1999</td>
<td>The Melissa worm was one of the first to automatically propagate via email</td>
</tr>
<tr>
<td>2016</td>
<td>Hacked American election?</td>
</tr>
</tbody>
</table>

### 2017’s Latest Trends in Cybercrime

- Politically-motivated attacks are on the rise
- Increased attention to public utilities being paid by foreign hackers
- Distributed denial of service (DDOS) attacks using the Internet of things (IoT)
- Increasing sophistication in spear phishing attacks
- Cyber criminals are using tools and techniques to make detection even more difficult
- Zero-day attacks are on the decline
Cybercrime Facts

- Cybercrime has recently surpassed illegal drug trafficking as a criminal money-maker
- A personal identity is stolen once every 3.1 seconds as a result of cybercrime
- Nearly half of all cybercrimes are committed against small businesses
- Exponential growth in the number of potential victims including: smartphones, cars, railways, planes, power grids, security cameras, refrigerators, garage door openers, etc.
- Some countries, including the UK, see cybercrime surpassing all other traditional crime

Crime-as-a-Service

- Growing industry of hackers for hire
- Hacking tools for sale
- Digital currency laundering services
- Hosting services designed for malware
- “Customer service” centers for ransomware
- The Dark Web is home to EBay-like clearing houses for a huge array of criminal services and products
Crime-as-a-Service – Dark Web

Digital Currencies

• Bitcoin is the most commonly used digital currency
• Relies on a decentralized ledger called a blockchain
• New Bitcoins are created through minting
• Pseudonymous
• Bitcoin exchanges buy/sell Bitcoins
• Price fluctuates with exchange rate

Today’s Exchange Rate: 1 Bitcoin = $4,638
Cybercrime is increasing

2016 saw a 40% increase in data breaches over 2015, and 2017 is expected to have a larger increase yet.

High cost of lost data

Data breaches cost on average $158 per lost record.
Huge global costs

Global cost of cybercrime is estimated to hit $2 trillion by 2019

Data loss happens fast…

68% of data breaches result in the loss of data within the first 24 hours
…but our response is slow

<2% of data breaches are discovered within 24 hours of occurring

Persistent threats

Attackers are in a network an average of 200 days before being detected
Reputation risk

Only 19% of breaches are self-detected by the compromised organization

COMMON TYPES OF CYBERCRIME
Business Email Compromise

- Targeted attack on a business
- Based on a compromise of legitimate business email account
- Relies on social engineering and/or data breach
- Mostly fraudulent wire transfers, but sometimes other forms of payment (checks)
- From January of 2015 to June 2016, there was a 1,300% increase in losses due to BEC
- Average loss is $130,000

BEC – Method 1

- Foreign Supplier
  - Victim is usually a business that has a long history and relationship with a foreign supplier
  - Fraudulent request is made for invoice payment to a different account
  - Email request will very-closely spoof legitimate request and will be difficult to identify as fraudulent
  - Sometimes also conducted by phone call or fax.
BEC – Method 2

- **Business Executive**
  - Email account of executive is either spoofed or hacked
  - Wire transfer request is made by the “executive” to another employee
  - Fraudulent request may also be made to the company’s financial institution
  - Request usually has an urgent nature

BEC – Method 3

- **Employee Email**
  - A business employee has their email hacked
  - Employee’s email history and contacts are studied
  - Fraudulent requests for payments are made to other businesses with whom the employee has relationships
BEC – Method 4

• Attorney
  – Fraudsters impersonate lawyers or representatives of law firms
  – Victims are pressured to act quickly and secretly
  – Funds transfers are requested
  – Usually happens late in the day

BEC – Method 5 (emerging)

• Data Theft
  – Business executive email is used
  – Victim is usually HR or payroll employee
  – Fraudulent request is usually for W-2 information or other personally identifiable information (PII)
  – First began happening in 2016
Preventing Business Email Compromise

- Educate and train employees
- Be wary of any urgent request or pressure to act quickly
- Develop processes for wire transfers that require multiple types of authorization
- Ensure all wire transfers correspond to an active purchase order in your system
- Purchase all domain names that are easily mistaken variants of your main domain name
- Create email rules that flag external email
- Sanitize websites and social media of sensitive information
- Do not allow the same employee to initiate and approve wire transfers
- If you are a victim, contact your financial institution and law enforcement immediately.

Ransomware

- Usually not targeted
- Victim data is encrypted and a ransom is demanded to decrypt data
- Ransom is paid via Bitcoin, wire transfers, and MoneyPak – all difficult or impossible to trace
- Numerous variants with more appearing regularly
- 167 times as much ransomware in 2016 compared to 2015
- Paying the ransom usually results in the decrypting of data
Ransomware (continued)

• Ransoms typically range from 1 or 2 bitcoins to 100 or more bitcoins
• FBI estimates $24 million was paid in 2015 (U.S.)
• For 2016, that number increased to nearly $1 billion
• Paying victims have included:
  − City and county governments
  − Police and Sherriff departments
  − School districts
  − Hospitals
  − International state governments
  − Businesses and organizations of all sizes
  − Home users
• Studies show that 64% of victims pay the ransom

Ransomware (continued)

• Average ransom per machine was $294 in 2015
• Average ransom per machine was $679 in 2016
• Over 400 variants in the wild at the end of 2016
• Currently the payload of choice for malicious email campaigns
• Ransomware toolkits are available on the Dark Web
• Relative anonymous nature of digital currency helps protect criminal activity
Ransomware Example – Locky (2016’s biggest)

All of your files are encrypted with RSA-2048 and AES-128 ciphers. More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To acquire your private key follow the steps:

If all of these addresses are not available, follow these steps:
1. Download and Install Tor Browser: http://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: timesa4.com/tim/sig7.png
4. Follow the instructions on the site.

!!! Your personal identification ID: 60CABB4005BF0AF !!!

Ransomware Example - PRISM

Your computer has been locked due to suspicion of illegal content downloading and distribution.

Illegal content found:

Collect data:

1. Your IP address
2. Your host name
3. Source of internet data
4. Location

Illegal content found:

MoneyPak
CVS
K
Walmart
Telus

Your case can be classified as computer-measured, according to 17 U.S. Code 612
That it may be closed without prosecution
Your computer will be deleted automatically.

In order to resolve this incident, you can contact us at the above-mentioned number.
Ransomware Example

![Ransomware Example](image1)

Ransomware Example - TeslaCrypt

![Ransomware Example - TeslaCrypt](image2)
Ransomware Example - Demonslay

I want to play...

Ransomware Example – Demonslay (continued)

I want to play a game with you. Let me explain the rules:
Your personal files are being deleted. Your photos, videos, documents, etc...
Don't worry! It will only happen if you don't comply.
However, I've already encrypted your personal files, so you cannot access them.
Every hour I select some of them to delete permanently, therefore I won't be able to access them either. They're gone for ever.
Are you familiar with the concept of exponential growth? Let me help you out.
It starts out slowly then increases rapidly.
During the first 24 hours you will only lose a few files, the second day a few hundred, the third day a few thousand, and so on.
If you turn off your computer or try to close me, when I start next time you will get 1000 files deleted. This is no joke, I'm very serious!
Yes you will want me to start next time, since I am the only one that is capable to restore your files. Don't wait till your pc stops working.
Now, let's start and enjoy our little game together!

59:35

1 file will be deleted.

Please, send at least $40 worth of Bitcoin here:
bc1q8w9b72h9v92m5j3v7f75r0d905k

Thanks a million, everyone included, my dear!
Ransomware Example – CryptoLocker

Your personal files are encrypted!

Your important files encryption is also encrypted on this computer; photos, videos, documents, etc. This is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.

The private key, which will allow you to decrypt the files located on a specific server, is encrypted in a binary format and is stored in a file called "Private Key". This key is also a one-time key. After that, anyone who has a copy of the private key will be able to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR. If the amount is not paid, the files will be deleted.

Click 'Next' to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Ransomware Example – CryptoWall

Your files are encrypted.

To get the key to decrypt files you have to pay 600 USD/600 EUR. If payment is not made, 600 USD/600 EUR will remain the cost of destroying files, which will increase every hour and will be 1000 USD/1000 EUR.

Prior to increasing the amount, 119h 59m 24s

Your system: Windows 7 32 bit
Purchased from: [Email address]
Total encrypted files: 5

[Recover] [Payment] [Exit] [Cancel] [Cancel]

We are presenting a special software - CryptoWall Decryption - which is able to decrypt and restore all of your encrypted files.

How to use CryptoWall Decryption?

1. Download the software from the official website.
2. Install the software on your computer.
3. Open the software and follow the on-screen instructions.
4. Enter your license key and file path.
Ransomware Example – CryptoWall variant

Is the content of the files that you have watched not readable?
It is normal because the files’ names, as well as the data in your files have been encrypted.

Congratulations!!!
You have become a part of a large community CryptoWall.

If you are reading this text that means that the software CryptoWall has removed from your computer

What is encryption?
Encryption is a reversible transformation of information in order to conceal the content and prevent unauthorized access. It is used to protect sensitive information and ensure the confidentiality of data.

In addition to the previous step, you need to decrypt the software with a key that you can decrypt your files and return everything to its place.

I almost understand what I have to do.

The first thing you should do is to read the instructions to the end.

You have a list of files encrypted with the CryptoWall software. The instructions tell you which files and which files have already been decrypted. They are your targets.

After reading this text, 100% of people turn to a search engine with the word CryptoWall where you find a lot of helpful advice and instructions. These solutions will not help you decrypt your files. Real experts often have a very special key to open them.

Any of your attempts to restore your files with these third-party tools can be fatal for encrypted files.

Note that changing data within the encrypted files 100% of software to recover files will, however, the data encryption software, you break encryption software that is the same as to collect a ransom. When you receive a ransomware, you have lost control over the file. You will not be able to pay the price, and also it is complete and irreversible. Using the software to restore files can make your files invisible to your system.

Remember that any intervention on the computer or software to restore files encrypted with this software may lead to the loss of your data.

In case of such cases, you are advised not to rely on help, and you will not be able to help you, and you will not be able to help you, and you will not be able to help you, and you will not be able to help you, and you will not be able to help you, and you will not be able to help you, and you will not be able to help you, and you will not be able to help you, and you will not be able to help you, and you will not be able to help you.

After purchasing the software package, you can.

Prepare for Ransomware

- It is not a matter of IF, but a matter of WHEN
- Excellent user training can help avoid problems
- Refine and restrict permissions to network files
- Frequent backups stored off-line
- Detection tools
- Test backup capabilities
- Get a Bitcoin wallet – just in case!

Prevent → Detect → Respond

©2017 RSM US LLP. All Rights Reserved.
Malvertising


• Online ads and videos
• Often displayed alongside reasonably-safe content
• Very easy for curious users to accidently click on
• Some malvertising doesn’t even require a click – it relies on vulnerabilities in Adobe Flash, etc.
• 4 to 5x increase per year
• Difficult to detect
• At times, exceeds ransomware detections
• “Kovter” is the most widely seen variant
Malvertising (continued)

Call for support: +1 (877) 640-6447
Call for support: +1 (877) 640-6447

I need help with...

Windows  

Windows Phone 8

Luna-Dowcoa

SOCIAL ENGINEERING
Social Engineering Definitions

Any act that influences a person to take an action that may or may not be in their best interest.

An attack vector that relies heavily on human interaction and often involves tricking people into breaking normal security procedures.

The art and science of getting people to comply with your wishes.

Using non-technical or low-technology means – such as lies, impersonation, tricks, bribes, blackmail, and threats – to attack information systems.

Hacking using brains instead of computer brawn.

Social Engineering

• Used to initiate or perpetuate a cybercrime
• Why do the hard work when someone else will do it for you?
• Relies on human psychology
• Human’s curiosity, greed, or willingness to help is used against them
• Most successfully-used vulnerability
• Most frequently-used exploit
Classic Example – Greeks and the Trojan Horse

- Source of the current security term, “Trojan horse”
- Relied on the Trojan’s human nature to bring the war trophy inside their gates
- That night, the hidden soldiers exited the horse and opened the gates of Troy, letting in the Greek soldiers

Classic Example - William Thompson

- Caused the term “confidence man” (con man) to be coined
- Operated in New York City in the late 1840s
- Simply asked people on the street if they would have confidence in him to hold their watch or money until tomorrow
  - People assumed he was an old acquaintance
Classic Example – Joseph “Yellow Kid” Weil

- Started out in the 1890s selling an Elixir that was mainly just rainwater
- Said, “A chap who wants something for nothing usually winds up with nothing for something”
- Often targeted bankers
- Sold fake claims to oil-rich land
- Swindled Benito Mussolini out of $2 million by selling land he didn’t own
- Sold talking dogs
- Stole over $8 million in his lifetime

Classic Example – Frank Abagnale

- Used Social Engineering to:
  - Defraud his father
  - Commit bank fraud
  - Impersonate professions:
    - Airline pilot
    - Teaching assistant
    - Doctor
    - Attorney

- Life story inspired the film, *Catch Me If You Can*, a Broadway musical, and an autobiography
Recent Example – Alcona County, Michigan

• Alcona County, Michigan treasurer embezzled $1.25 million of the county’s $4 million operating budget in 2007
• Used the money to pay a 419 scammer
  – Nigerian prince
  – Spanish prisoner
• The treasurer believed the emails from the scammer
• Received 14 years in prison

Recent Example - Target

• One of the largest attacks of 2013
• Hackers stole 40 million credit card numbers from POS systems
• Attackers gained access by using a phishing email sent to Target’s HVAC subcontractor
• Illustrated that the weakest link can be a third-party contractor, supplier, or partner
Real World Examples

- Small Town

Personal Example

This is a payment confirmation e-mail for the ticket you ordered on Delta.com website.

Your credit card has been charged.

Flight Number: WA618348
Date: MAR 7 2017, 17:45 CDT
Departure: Washington, DC

You can download and print your ticket from our website:
https://www.delta.com/tickets/viewTicket.do?order_id=70126742&flight=W618348

For more information regarding your order, contact our technical support by visiting:
https://www.delta.com/content/faqs/en_US/support.html

Thank you for flying with Delta Airlines.
©2017 Delta Air Lines, Inc.
Social Engineering may have changed the world

Types of Social Engineering

- Pretexting
- Diversion
- Phishing
- Vishing / Phone Phishing
- Spear Phishing
- Water Holing
- Baiting
- Quid Pro Quo
- Tailgating
Types of Social Engineering - Pretexting

- Social engineer creates a fabricated scenario
- May pose as a representative of a legitimate business that needs sensitive information
- False sense of trust created
- Can involve physical element – showing up and pretending to be someone they are not

Types of Social Engineering - Diversion

- Social engineer tricks the victim into delivering goods or data to an unsafe location
- Common con in the physical world where delivery drivers are told to change the delivery to a place “around the corner”
- Persuades victim to send data to a location that results in theft of data
Types of Social Engineering - Phishing

- Most common form of social engineering
- Social engineer sends an email to a huge list of potential victims
  - Estimated that 200 million are sent each day
  - 15 million of which make it through spam filters
  - Around 1/3 of those are opened
  - 12% of those opening messages click on the links
  - 10% of those who clicked share their information (about 80,000 people per day)
- Email attempts to look like legitimate correspondence from a bank, credit card company, PayPal, Ebay, etc.
- Malicious code in the email
- Directs victim to a fake site where credentials are stolen
- Downloads and installs malware / ransomware

Types of Social Engineering – Vishing (Phone Phishing)

- Phishing using a telephone
  - Real human caller
  - War dialer
- Victims receive phone calls from social engineers attempting to steal personal data or money
- May use caller ID spoofing
- Inbound vishing uses sophisticated IVR systems
- Close cousin – “smishing” uses the same concept, but with text messaging (SMS)
Types of Social Engineering – Spear Phishing

- Targeted phishing / vishing
- Social engineer does research to make phishing attempts more successful
  - Company website
  - Blogs
  - Social media
- Spear phishing is often how business email compromise starts
- Goal is the same as with phishing:
  - Steal credentials
  - Install malware for further attacks

Types of Social Engineering – Water Holing

- Social engineers target an industry, interest group, organization, etc.
- Website commonly used by victims is studied and ultimately compromised
- Malicious code is delivered to users who visit the site
- Code is used to gain access into victims’ computers
Types of Social Engineering – Baiting

- Social engineer lures the victim into opening a malicious file, usually relying on curiosity or greed
- Physical media is often used
- Left in bathrooms, parking lots, break rooms, elevators, etc.
- Online forms of baiting include malvertising, free downloads, etc.
- Payload usually gives attackers access to victims’ computers

Types of Social Engineering – Quid Pro Quo

- Social engineer tricks the victim into doing something in exchange for a service or action
- Similar to baiting
- Often the social engineer poses as a company IT person and asks the victim to perform some action in order to upgrade their system
Types of Social Engineering – Tailgating

- Typically a physical method of social engineering
- Social engineer gains physical entry to a secure area
- Follows a legitimate employee
- Asks an employee for entry because they forgot their badge
- Poses as a delivery driver with many boxes and asks to have door held

Stopping Social Engineering

- Train employees
- Train employees
- Test employees

- Maintain as good security on all the “technical parts” of the environment as absolutely possible
ANATOMY OF THE ATTACK

An Elite Club

- Ashley Madison
- Yahoo
- LinkedIn
- Verizon
- The IRS
- Wendy’s
- The White House
- T-Mobile
- CIA Director
- HBO
- Target
- US OPM
- Sony
- JP Morgan Chase
- iCloud / Apple
- The FBI
- Home Depot
- Anthem Insurance
- Yahoo (again)
- Comcast
- Equifax
- WTO
- Staples
- (your name here)
Anatomy of the Attack

1. Phishing and zero day attack
2. Backdoor
3. Lateral movement
4. Data gathering
5. Exfiltration

WHAT CAN YOU DO?
Three basic steps to prevent cybercrime

1. Get Real
2. Get Help
3. Get Educated

1: Get Real

- Understand and appreciate the threats that exist
- Make cybersecurity an organizational priority from the board/CEO/owner down
- Never assume safety from anonymity, size, or geography
- Know that information security is a never-ending project
- Recognize that you may be outnumbered but you don’t have to be outsmarted
2: Get Help

- Unless you are a huge company, you most likely cannot adequately handle all information security functions internally
- Perform security review, audit, assessment, etc., even if not required by regulation
- Enlist a vendor to assist with patch management, anti-virus, etc.
- Order regular penetration tests and social engineering tests

3: Get Education

- Subscribe to cybersecurity newsletters and feeds
- Keep cybersecurity a top-of-mind subject throughout the organization
- Provide cybersecurity and social engineering training to employees
- Test employees for adherence to cybersecurity standards
- Understand what rights users have to network resources
CLOSING THOUGHTS

An ounce of prevention…

99.9% of vulnerability exploits occur more than a year after the vulnerability was disclosed.
...is 10 patches away

97% of exploits occurred from a list of just 10 published vulnerabilities

Humans...

30% of recipients now open phishing messages
…often the weakest link

12% of recipients **click on** phishing attachments

Too many privileges

55% of insider incidents involve abuse of privileges
Passwords!

39% of passwords are only 8 characters long and can be cracked in under one day.

Questions and answers?