Cybercrime Trends

2019 Update

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

We promise to know you and help you.

Current State of Affairs

What are the bad guys up to?

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Hackers have “monetized” their activity

- More hacking
- More sophistication
- More “hands-on” effort
- Smaller organizations targeted

Current State of Affairs

Organized Crime

- Wholesale theft of personal information

Ransomware

- Holding your data hostage

Payment Fraud

- "Corporate Account Take-Over" - aka CATO
- Use of credentials to commit online banking and credit card fraud

Credential "Harvesting"

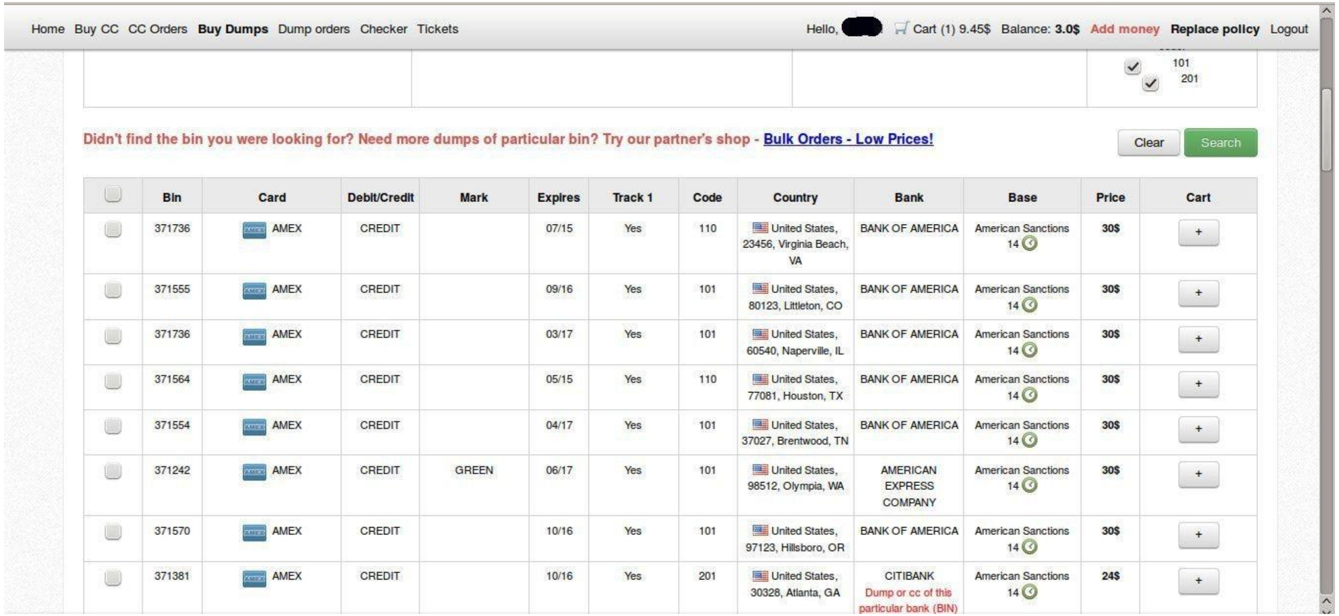
Organized Crime

Current State of Affairs

Hacking is run like a business with different departments

- Writing malware
- Sending phishing emails
- Stealing data
- Selling data
- Conducting payment fraud
- Etc.

Current State of Affairs


Home Buy CC CC Orders Buy Dumps Dump orders Checker Tickets
Hello, [redacted]
Cart (1) 9.45$ Balance: 3.0$ Add money Replace policy Logout
☑ 101
☑ 201
Clear
Search

Didn't find the bin you were looking for? Need more dumps of particular bin? Try our partner's shop - Bulk Orders - Low Prices!

□	Bin	Card	Debit/Credit	Mark	Expires	Track 1	Code	Country	Bank	Base	Price	Cart
□	371736	AMEX	CREDIT		07/15	Yes	110	United States, 23456, Virginia Beach, VA	BANK OF AMERICA	American Sanctions 14	30$	+
□	371555	AMEX	CREDIT		09/16	Yes	101	United States, 80123, Littleton, CO	BANK OF AMERICA	American Sanctions 14	30$	+
□	371736	AMEX	CREDIT		03/17	Yes	101	United States, 60540, Naperville, IL	BANK OF AMERICA	American Sanctions 14	30$	+
□	371564	AMEX	CREDIT		05/15	Yes	110	United States, 77081, Houston, TX	BANK OF AMERICA	American Sanctions 14	30$	+
□	371554	AMEX	CREDIT		04/17	Yes	101	United States, 37027, Brentwood, TN	BANK OF AMERICA	American Sanctions 14	30$	+
□	371242	AMEX	CREDIT	GREEN	06/17	Yes	101	United States, 98512, Olympia, WA	AMERICAN EXPRESS COMPANY	American Sanctions 14	30$	+
□	371570	AMEX	CREDIT		10/16	Yes	101	United States, 97123, Hillsboro, OR	BANK OF AMERICA	American Sanctions 14	30$	+
□	371381	AMEX	CREDIT		10/16	Yes	201	United States, 30328, Atlanta, GA	CITIBANK Dump or cc of this particular bank (BIN)	American Sanctions 14	24$	+

https://www.deepdotweb.com/wp-content/uploads/2014/10/listings.jpg

Ransomware

Current State of Affairs

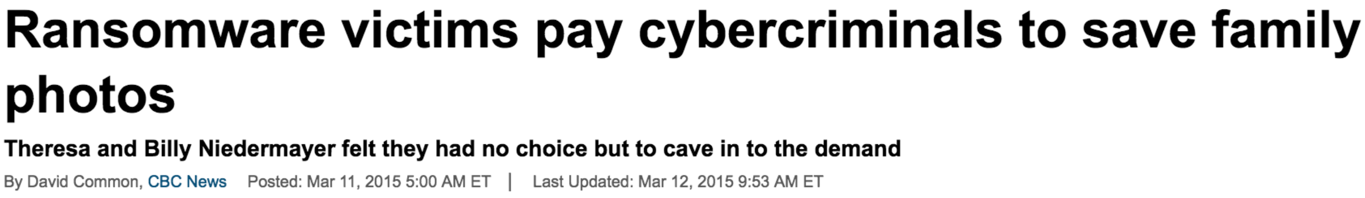
- CryptoWall, CryptoLocker, wannacry, petya, etc.
- Encrypt all data, hold it “ransom” for $$
  - Data on local machine and on network
- Attackers are putting much more time and effort into these types of attacks over the last year
- Starting to target other operating systems, like Macs

3 Generations

1. Local machine only
2. Local machine plus network permissions
3. Local machine plus ***ENTIRE NETWORK***

Ransomware

Current State of Affairs



Ransomware victims pay cybercriminals to save family photos

Theresa and Billy Niedermayer felt they had no choice but to cave in to the demand

By David Common, CBC News Posted: Mar 11, 2015 5:00 AM ET | Last Updated: Mar 12, 2015 9:53 AM ET

"Theresa and Billy Niedermayer paid an **$800** ransom to get precious family photos of their three young boys back from cybercriminals."

http://www.cbc.ca/news/technology/ransomware-victims-pay-cybercriminals-to-save-family-photos-1.2962106

Payment Fraud

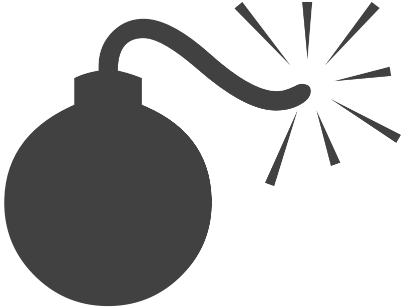
Current State of Affairs

- Public School
- Hospice
- Municipal Government (City)
- Main Street newspaper stand
- Electrical contractor
- Health care trade association
- Rural hospital
- Mining company
- On and on and on and on…………….

Payment Fraud

CATO – 3 Versions

1. Deploy malware – keystroke logger
2. Deploy malware – man in the middle
3. Recon/email persuasion
    1. ***"Whaling"***
    2. ***Business email Compromise***
    3. ***CEO attack***
        1. ***NEW – W2 attacks***

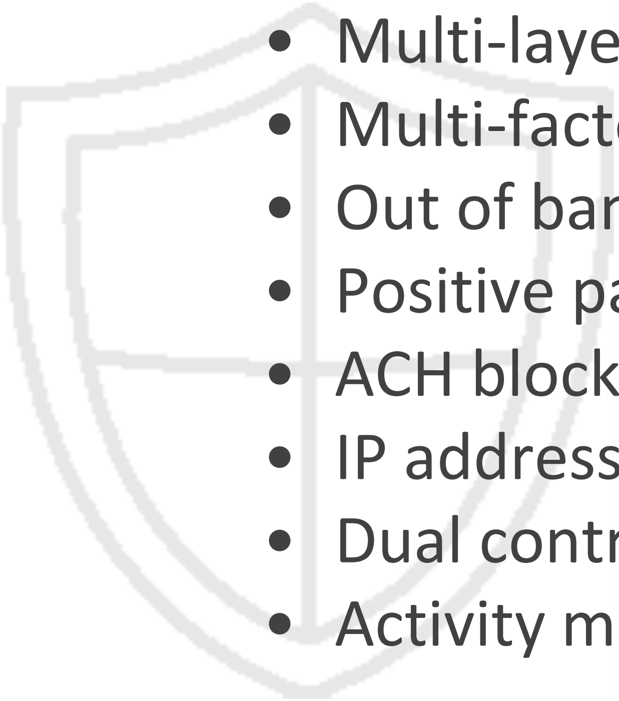


Multi-Factor Authentication Solutions

- MFA is critical
- Silver bullet?
- Text msg?

Payment Fraud

CATO Defensive Measures



- Multi-layer authentication
- Multi-factor authentication
- Out of band authentication
- Positive pay
- ACH block and filter
- IP address filtering
- Dual control
- Activity monitoring

Credential Harvesting

Credential Harvesting

- Driven by movement to the cloud
- Malware
- Social engineering

Payment Fraud

Mitigation Keys

- Train users regarding email phishing
- Maintain current patch levels
- Remove local administrators
- ***Maximize relationship with the bank***
- ***Isolate the PC used for online banking***
- Implement breach monitoring/ incident response
- Use MFA for all cloud apps

Current State of Affairs

The Cost

Global cybercrime cost business up to:
$400 **BILLION** annually

Some companies theorize it will reach:
$2.1 **TRILLION** by 2019

> “There are only two types of companies: Those that have been hacked and those that will be. Even that is merging into one category: those that have been hacked and will be again.”
>
> - Robert Mueller

Questions?

Mark Eich

Principal

Information Security

mark.eich@claconnect.com

***

(612)397-3128

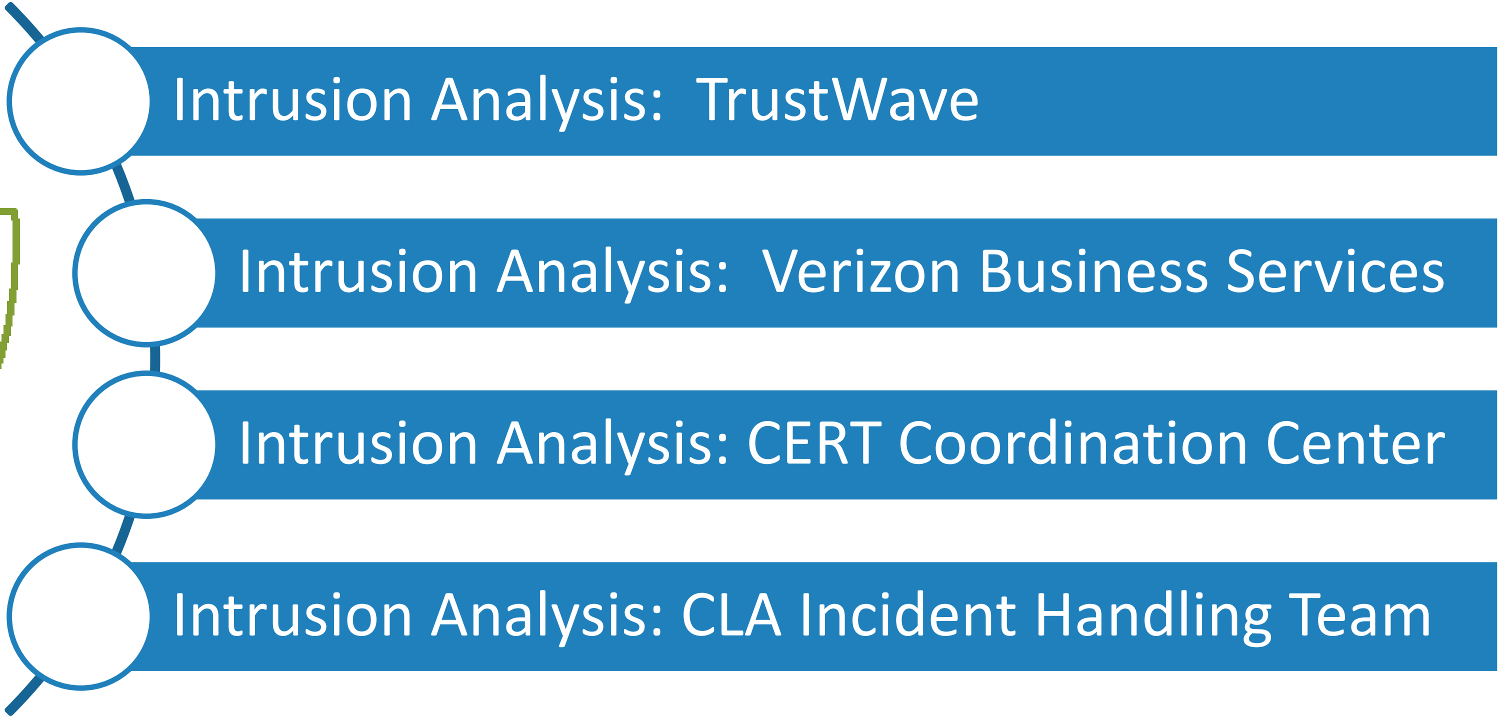
10 Key Defensive Measures

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

We promise to know you and help you.

96% of Attacks are Preventable!



Intrusion Analysis: TrustWave

Intrusion Analysis: Verizon Business Services

Intrusion Analysis: CERT Coordination Center

Intrusion Analysis: CLA Incident Handling Team

Strategies

Our information security strategy should have the following objectives:

- Users who are more aware and savvy
- Networks that are resistant to malware
- Relationship with our financial institution is maximized

Ten Keys to Mitigate Risk

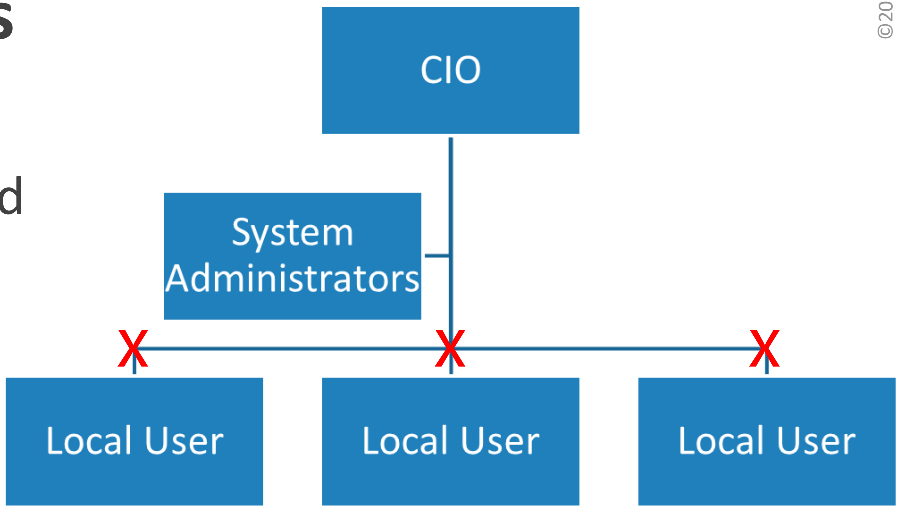
1. Strong Policies -

- Email use
- Website links
- Removable media
- **Users vs Admin**

Ten Keys to Mitigate Risk

2. Defined user access roles and permissions

- Principal of minimum access and least privilege
- **Users should NOT have system administrator rights**
  - **"Local Admin" in Windows should be removed (if practical)**



Ten Keys to Mitigate Risk

3. Hardened internal systems (end points)

- Hardening checklists
- Turn off unneeded services
- **Change default password**
- **Use Strong Passwords**
- **Consider application white-listing**

4. Encryption strategy – data centered

- Email
- Laptops and desktops
- Thumb drives
- **Email enabled cell phones**
- Mobile media

Ten Keys to Mitigate Risk

5. Vulnerability management process

- Operating system patches
- **Application patches**
- Testing to validate effectiveness –
  - “belt and suspenders”

Ten Keys to Mitigate Risk

6. Well defined perimeter security layers

- **Network segments**
- Email gateway/filter
- Firewall – "Proxy" integration for traffic in AND out
- Intrusion Detection/Prevention for network traffic, Internet facing hosts, AND workstations (end points)

7. Centralized audit logging, analysis, and automated alerting capabilities

- Routing infrastructure
- Network authentication
- Servers
- Applications
- Know what "normal" looks like…

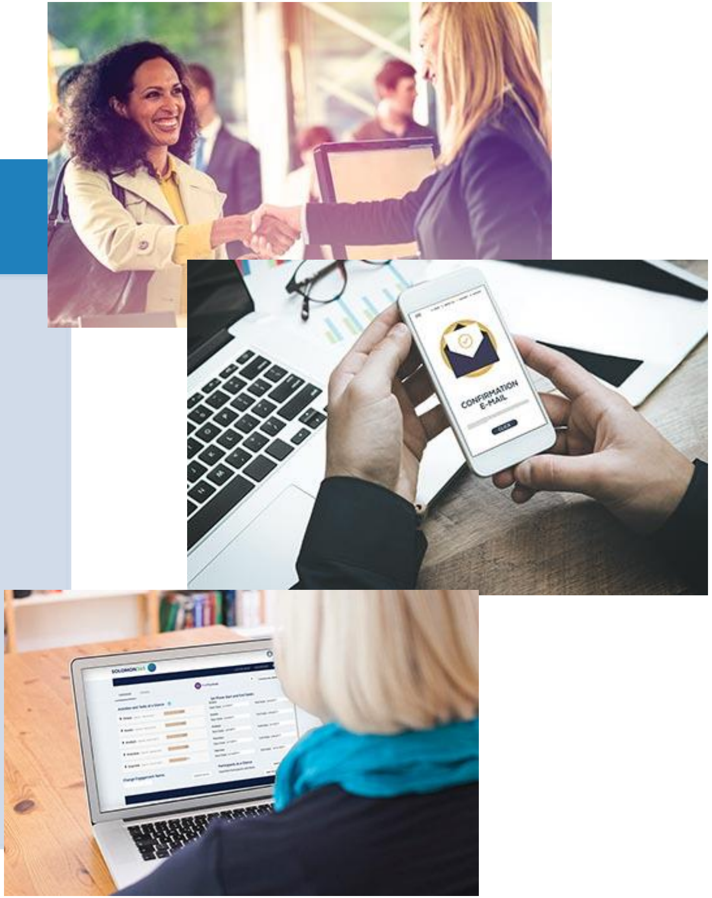
Ten Keys to Mitigate Risk

8. **Defined incident response plan and procedures**
   - **Be prepared**
   - Including data leakage prevention and monitoring
   - Application whitelisting
   - Forensic preparedness
   - Insurance
   - Practice…

Ten Keys to Mitigate Risk

9. Know/Use Online Banking Tools

- Multi-factor authentication
- Dual control/verification
- Out-of-band verification/call-back thresholds
- ACH positive pay
- ACH blocks and filters
- Review contracts relative to all these
- Monitor account activity ***daily***
- **Isolate the PC used for wires/ACH**



Ten Keys to Mitigate Risk

10.
Test
Test
Test

- “Belt and suspenders” approach
- Penetration testing
  - ◊ Internal and external
- Social engineering testing
  - ◊ Simulate spear phishing
- Application testing
  - ◊ Test the tools with your bank
  - ◊ Test internal processes