Cybersecurity for Municipalities

CML

2015 Webinar Series

Overview

- Intro – CGAIT
- Today's Landscape
- Case Studies
- Operational Considerations
- Questions

Panelists

Ned McClain
AppliedTrust, Inc.

Tom Charkut
City of Lakewood

Ken Price
City of Littleton

CGAIT

Colorado Government Association of Information Technology

Mission

To promote advances in information technology in order to facilitate networking, collaboration, cooperation and education among government information technology leaders within Colorado resulting in greater efficiencies and effectiveness for member organizations while enhancing services to Colorado communities and its citizens.

CGAIT

Colorado Government Association of Information Technology

Purpose

- *To assure the most cost-effective use of information technology resources CGAIT has been formed to promote statewide and regional cooperation.*
- *To provide education and information for non-IT County/City officers on technology initiatives, as well as the roles, responsibilities and requirements of Information Technology organizations.*
- *To foster shared services between members as a means to reduce costs and increase efficiencies.*

CGAIT

Colorado Government Association of Information Technology

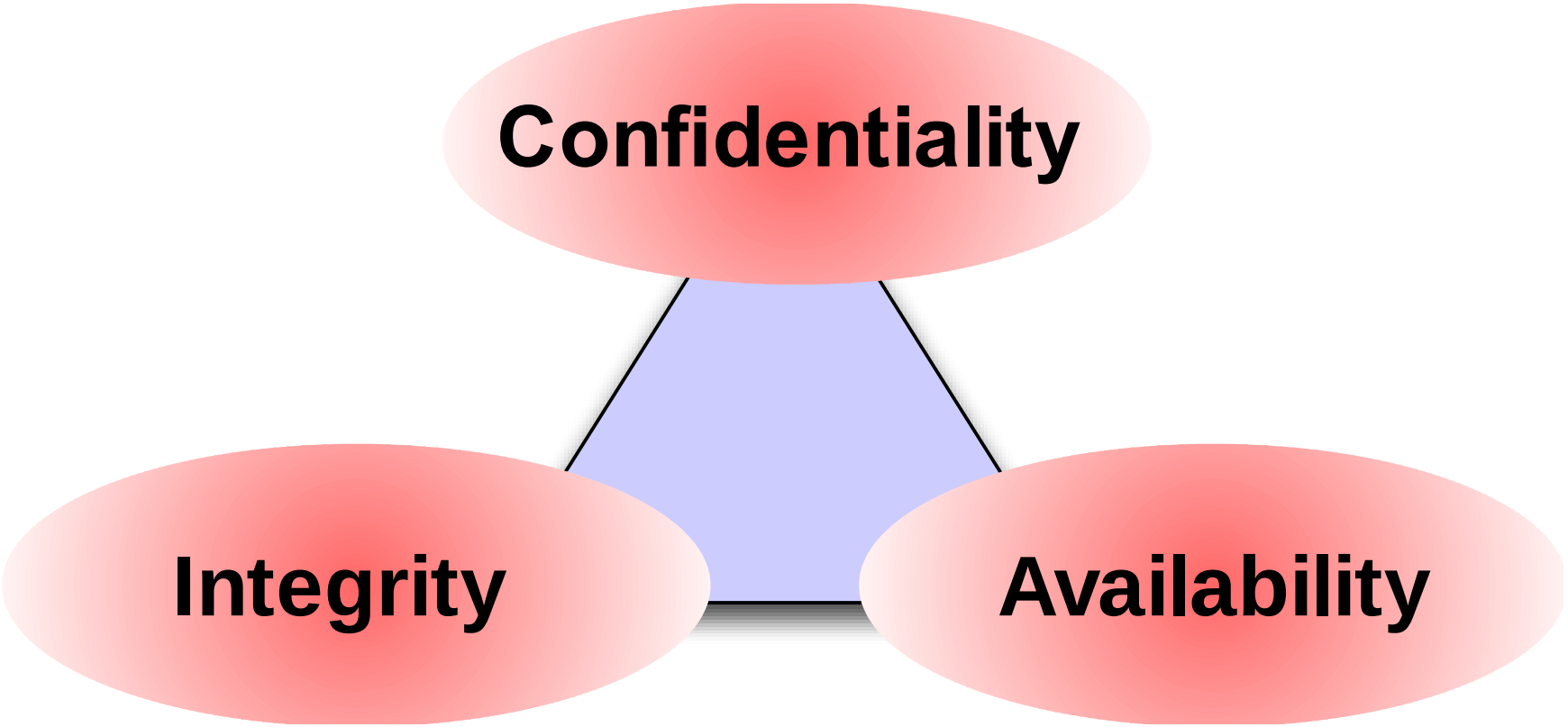
Purpose

- *To share the knowledge and experience of members, as appropriate, with governmental and non-governmental entities for the purpose of improving the quality of technology discussions and decisions that affect citizens and society.*
- ***Serve as an advisory body to the Colorado Municipal League, Colorado Counties Incorporated, and other non-IT organizations in Colorado.***

Today's Landscape

- Security
- Compliance

Holistic Security



3 risks and 3 priorities:

Disclosure -> Confidentiality
Corruption -> Integrity
Unavailability -> Availability

PII

PII

Name
Social Security Number
Cardholder, Financial Data
Protected Health Information (PHI)
Face, fingerprints, or handwriting
Any location data
Birthday, place, age
Vehicle registration
Driver's license number

Security Crisis Case Studies

- Real Colorado incidents in 2014
- Names have been changed to protect the “innocent”
- What can we learn from their experiences?

SuperCounty – Parks and Rec

- **Besides traditional parks and recreation centers, SuperCounty has a dozen community Spa and Massage centers. At only $5/hour, the centers are popular!**

- **SuperCounty uses a PCI-approved point-of-sale system, so they don't have to worry about PCI compliance.**

Signs of Trouble

- One morning, the finance staff gets a call from American Express…

  "We are investigating you as a CPP"

- **All credit card transactions frozen** until SuperCounty proves PCI compliance

What happened?

- *EVERY* organization that touches credit cards must be PCI compliant
- Complete a PCI SAQ today, enjoy safe harbor tomorrow!
- Know the scope of ALL of your compliance requirements:
  - **PCI DSS**
  - **NERC CIP (SCADA)**
  - **HIPAA**
  - **CJIS**
  - **FERPA**
  - **Red Flag Rule**
  - **FedRAMP**
  - **CORA**
  - **COPPA**
  - **FISMA and NIST**

EastWestSlope, Colorado

- Medium-sized municipality that generally makes appropriate investments in IT.
- Legacy email and filesharing have served them well, so no pressure for change.

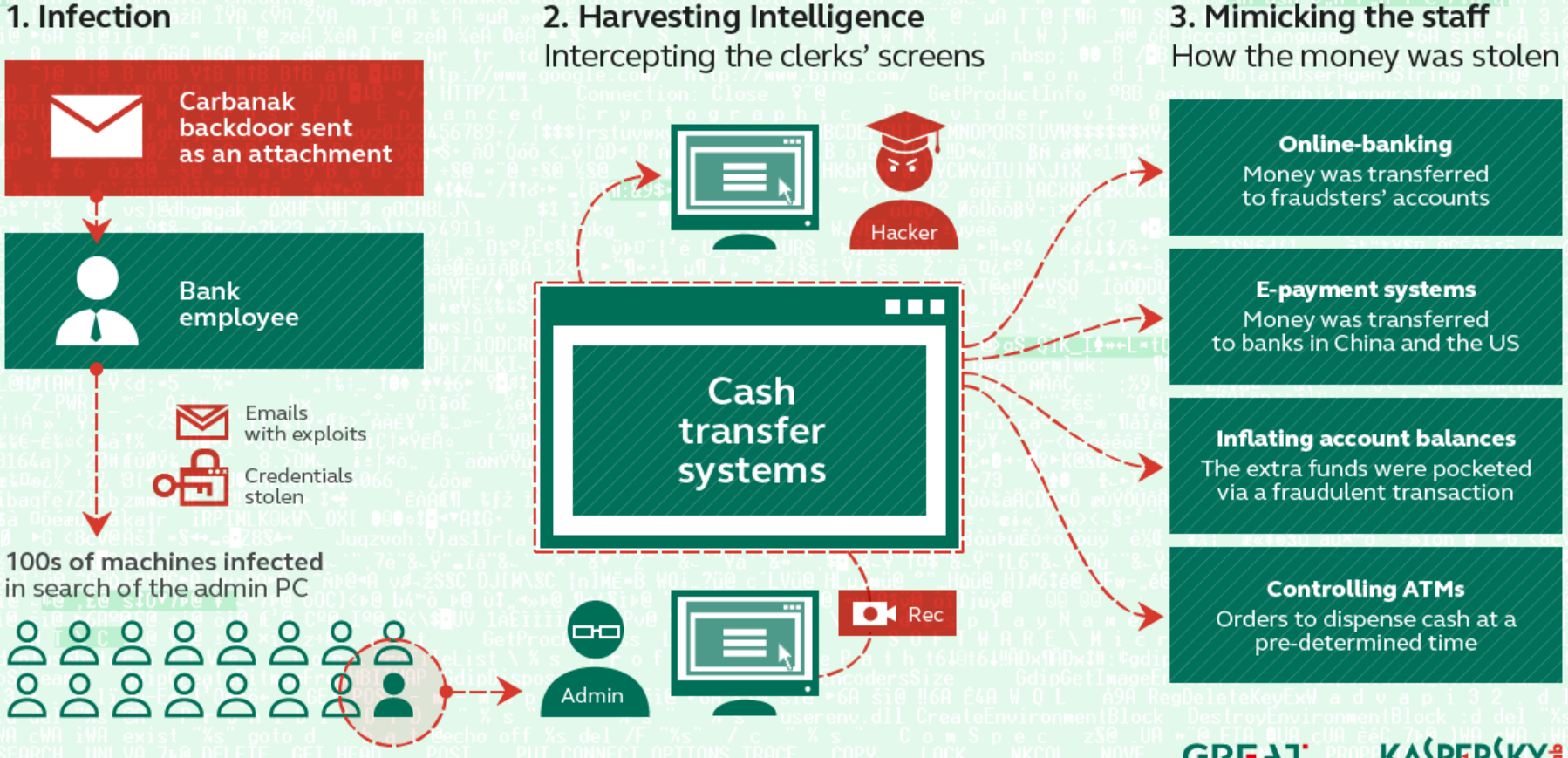
Signs of Trouble

- Mid-morning, IT HelpDesk starts receiving automated alerts of application failures.
- Users begin calling the helpdesk complaining of access problems.
- Eventually, one end-user calls in saying there is a weird message on their computer…


CryptoLocker
Your personal files are encrypted!
Your important files encryption produced on this computer: photos, videos, documents, etc. Here 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 single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never 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 / similar amount in another currency.
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.
Private key will be destroyed on
10/9/2013
4:25 PM
Time left
95 : 56 : 35
Next >>
Malwarebytes

How the Carbanak cybergang stole $1bn

A targeted attack on a bank



Your computer has been locked due to suspicion of illegal content downloading and distribution.
Mentioned illegal content (414 Mb of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal Laws:

18 U.S.C. § 2251- Sexual Exploitation of Children (Production of child pornography)
18 U.S.C. § 2252- Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)
18 U.S.C. § 2252A- certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to $250,000.

Technical details:
Involved IP address: [redacted]
Involved host name: [redacted]
Source or intermediary sites: http://pornerbros.com

All suspicious files from your computer were transmitted to a special server and shall be used as evidences. Don't try to corrupt any data or unblock your account in an unauthorized way.

Your case can be classified as occasional/unmotivated, according to title 17 (U. S. Code) § 512. Thus it may be closed without prosecution. Your computer will be unblocked automatically.

In order to resolve the situation in an above-mentioned way you should pay a fine of $300.

HOW TO UNLOCK YOUR COMPUTER:

1 Take your cash to one of this retail locations:
Walmart, Kmart, Sam's Club, 7-Eleven, CVS pharmacy, Walgreens

2 Get a MoneyPak and purchase it with cash at the register
MoneyPak

3 Come back and enter your MoneyPak code to unlock your computer (5 attempts available)

Code: Submit

1 2 3
4 5 6
7 8 9
Delete 0 Enter

Permanent lock on 05/01/2013 5:20 p.m. EST

What happened?

- The end-user opened an email attachment containing ransomware.
- Legacy file sharing allowed one compromised workstation to destroy files organization-wide.
- Not all directories were backed up – massive data loss.

Lessons learned

- Every user has real responsibility for security
  - Annual training just doesn't cut it.
- Legacy "J: drive" fileshares are not a secure going-forward solution
- Backups, backups, backups*

* **tested** backups!

PrettyGreat Planning Department

- PGPD staff provide weekly home visits for under-construction homes, or anyone who needs a lightbulb changed or handyman!

- Each planner records their sessions on a work laptop, including private details about home maintenance.

Signs of Trouble

- While picking up a sandwich for lunch, a planner's laptop is stolen from their car!

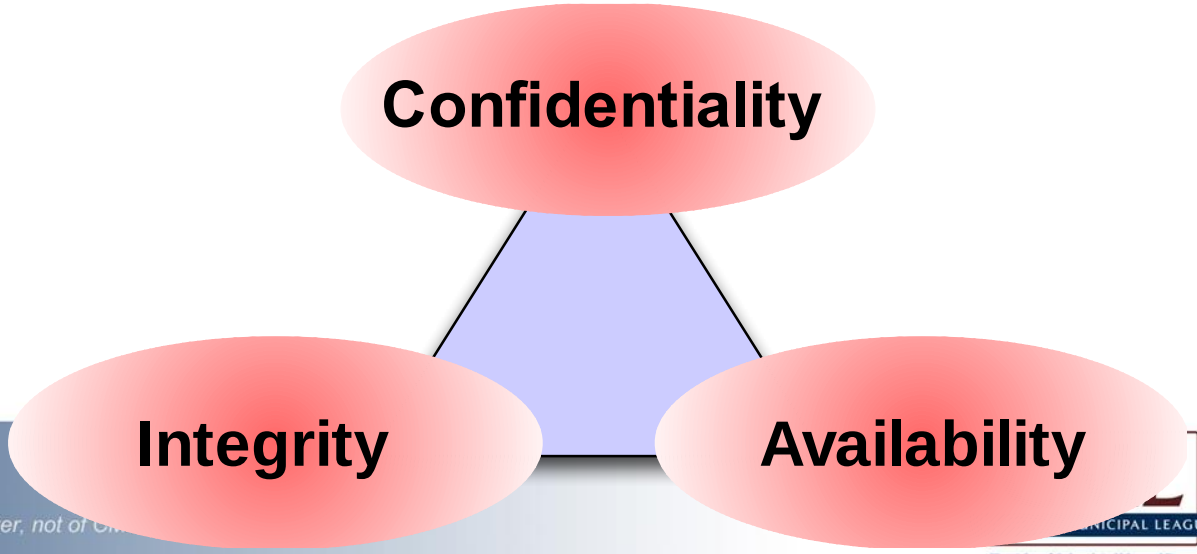
What happened?

- Due to privacy legislation, PGPD must notify all citizens whose data might have been on the laptop, **as well as the press!!**

- Lots of important data is simply unrecoverable!

Lessons learned

- Ensure all laptops enable disk encryption
- Remember that confidentiality is only part of security
  - (perform and test your backups!)



SnowyTown, Colorado

- SnowyTown struggles for IT budget, but recently invested in secure wireless for several critical facilities.
- Because secure wireless is expensive to deploy (and maintain!), SnowyTown doesn't offer wireless for several smaller facilities.

Signs of Trouble


9NEWS

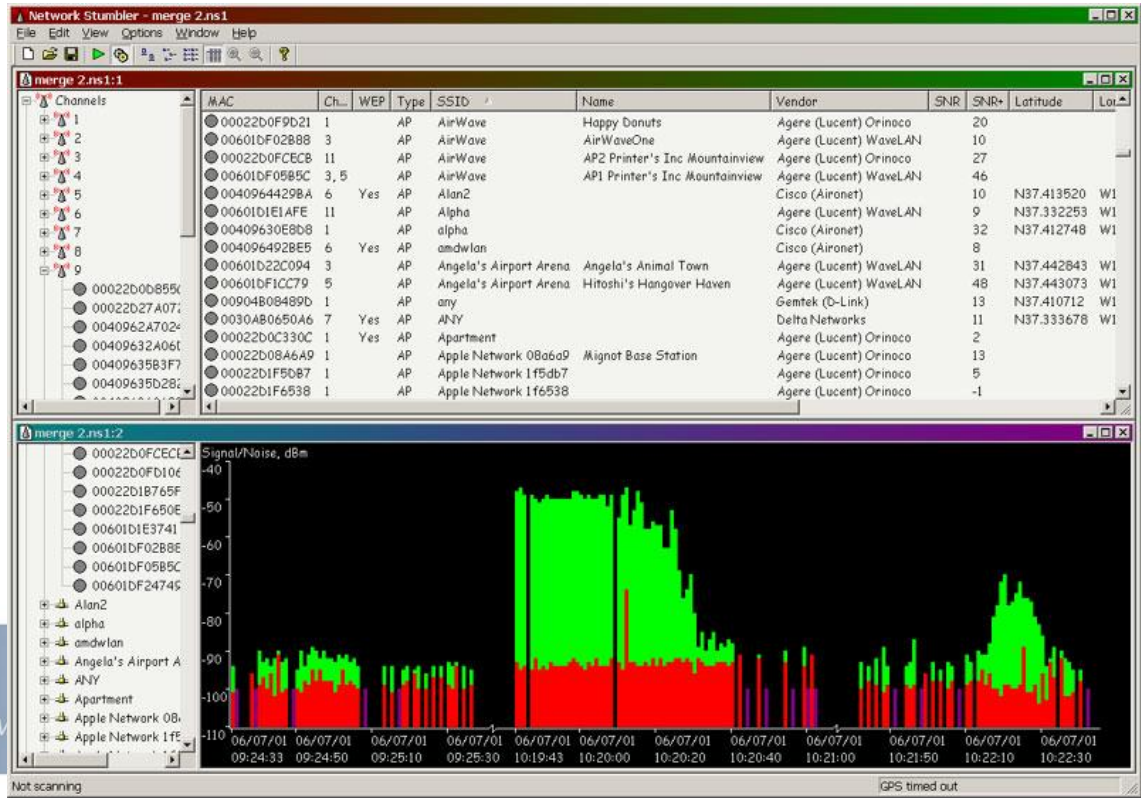
What happened?

- Tired of not being able to work in the conference room, a worker in one of the smaller facilities installed a cheap WAP from Staples under their desk.

- The entire SnowyTown network was exposed to the parking lot!

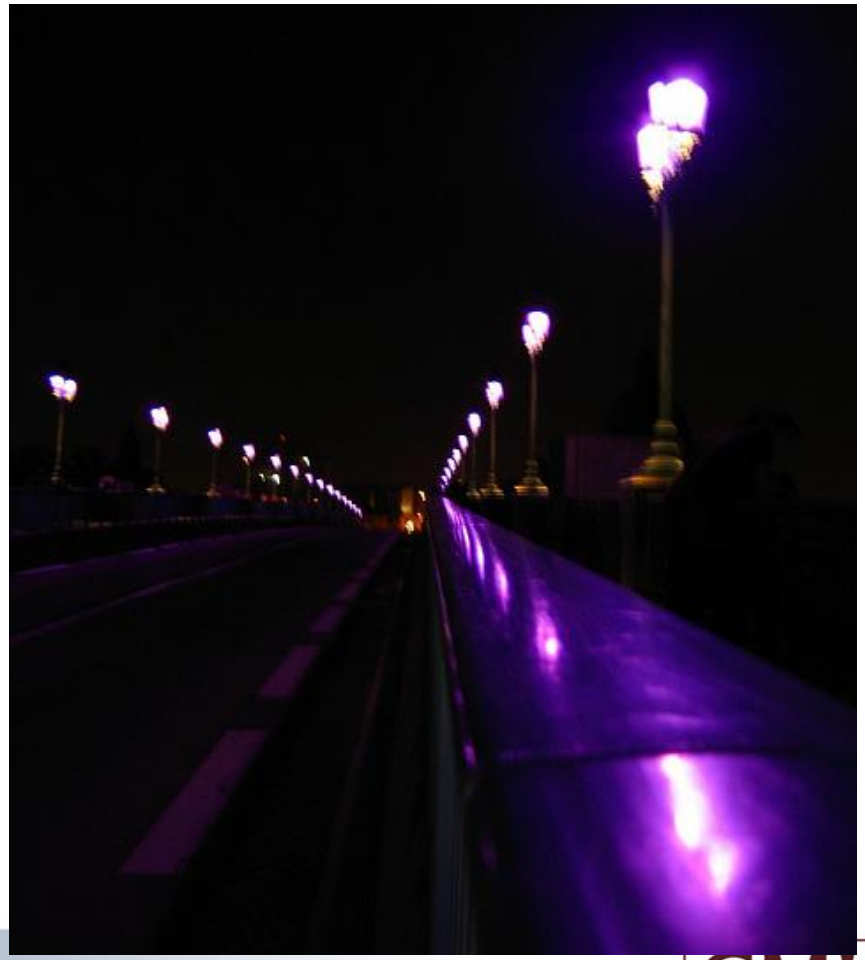
Lessons learned

- Every organization needs a simple, accessible IT security policy.
- Perform regular wireless walkthrough audits.
- Have a guest wireless plan.



Anytown Public Works

- The citizens of AnyTown, Colorado, have voted for the important mission of replacing yellow street lights with purple ones.
- All utility payments are outsourced to PayPal, so they are secure!
- Accounting team skimmed over PayPal logs every day just to be sure things looked ok.



Signs of Trouble

- During weekly accounting reconciliation, a gigantic discrepancy is found in the PayPal balance:

$280,000

What happened?

Upon closer inspection, **many** $9999 payments were timed to occur during the morning batch process.

What happened?

- Somehow, the PayPal account was compromised.
- With many staff sharing the same PayPal login, it was very hard to track down how the password was initially stolen.
- Some staff occasionally worked from home, from old unsecured computers.
- FBI, CBI, Denver Police, PayPal Fraud Dept all refused to offer meaningful assistance.

Lessons learned

- Never share logins!
  - Always have “individually-identifiable access”
  - Change all passwords when someone leaves the organization
  - Force password changes at least quarterly
- Establish relationships with law enforcement **before** an incident.
- Consider Cyber Insurance.

SmallTown IT Department

- Small team of super-smart IT cowboys.
- “At our size and skills, process and documentation just slow us down.”
- Everyone is excited about the smart new hire.

Signs of Trouble

- Late one night, a system admin notices a strange account
- With no one else in the office, the system admin decides the server must have been hacked
- The decision is made to shut down the website until the path of attack is discovered
- Several team members login and “look around” for evidence of an attack

What happened?

- The site was down for 16 hours before the source of the account was discovered

- John, a senior sysadmin, added the account yesterday, before going on vacation!

Lessons learned

- Every organization should be following basic IT change practices

- Every organization needs a simple, accessible incident handling guide
  - Triage
  - Communication
  - Escalation

Operational Considerations

- Budgeting
  - Range between 8% and 20% of IT spend
    - Operational
      - Maintenance hardware, software
      - Labor
        - » Consider consultants
    - Capital
      - Large purchase items / projects to achieve goals

Operational Considerations

- Cyber Insurance
  - New type
  - Cyber Liability
  - Network & Information Security Liability
  - Crisis Management
  - Security Breach Notification
  - Limits & deductibles organization-specific

Questions to Ponder

Wireless Services

Do we have strategy for community/guest wireless? Are we performing regular audits for rogue access points?

Compliance

Do we have an up-to-date understanding of applicable standards and requirements? Are we doing everything possible to minimize our scope?

Cross-functional Security Team

Have we created a security team that represents technologists, HR, legal, and the interests of end users?

Questions to Ponder

Incident Handling Guide

Is a printed security incident handling guide available to all levels of staff?

Mobile Device Strategy

Do we have a plan for securing mobile devices, including those owned by users?

Awareness and Training

Do we regularly remind all staff that they are the most critical link the security chain?

Questions & Discussion