RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: GRC-T10

A Comedy of Errors: Assessing and Managing the Human Element of Cyber Risk

R Jason Straight

Sr. VP, Chief Privacy Officer
UnitedLex Corp.

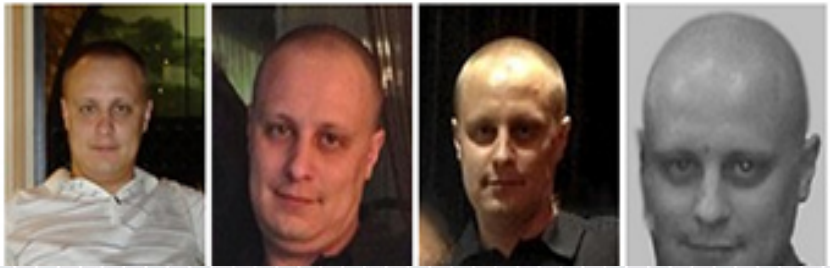
Has anyone seen this man?

FBI offers $3 million reward for Russian ‘cyber fugitive’

WANTED
BY THE FBI

Conspiracy to Participate in Racketeering Activity; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Bank Fraud; Wire Fraud; Money Laundering; Aggravated Identity Theft

MIKHAILOVICH BOGACHEV



The Telegraph

Russian hacker wanted by US hailed as hero at home

UnitedLex

We're getting warmer . . .

Responsible for theft of $40M credit/debit cards?

Insider Threats

Don’t turn your back on this notorious crew!

RSA Conference2015
San Francisco | April 20-24 | Moscone Center

UnitedLex

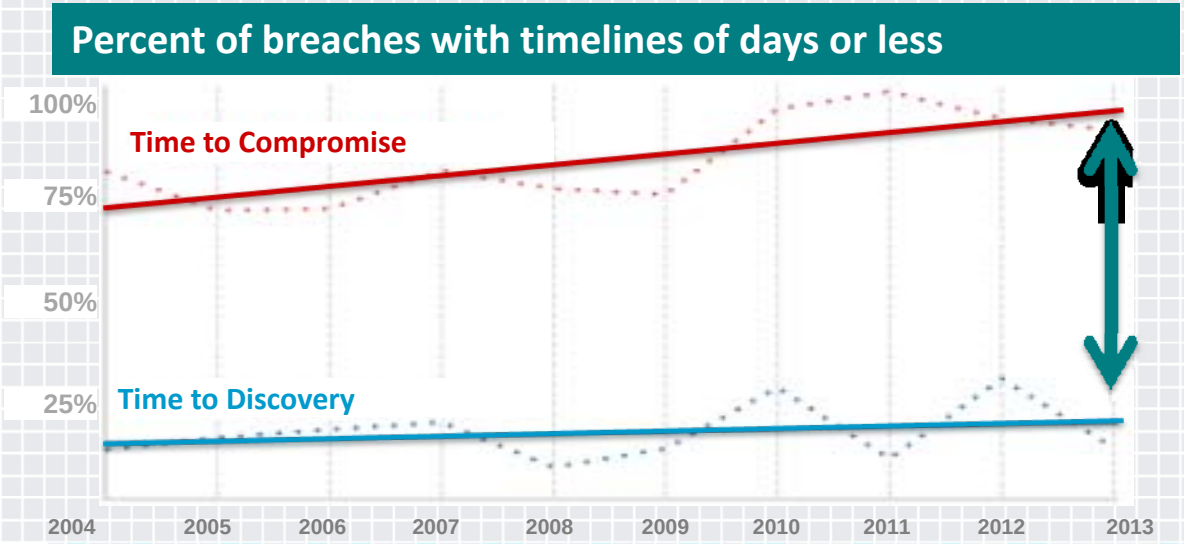
Introduction

Objectives

- Suggest that we are focusing our security resources on the wrong things
- Illustrate the ways insiders create risk
- Introduce ways to reduce insider risks and create a culture of security

Trends and Developments

Gap between offense and defense is growing — despite huge investments by defenders



SOURCE: 2014 Verizon Data Breach Investigations Report

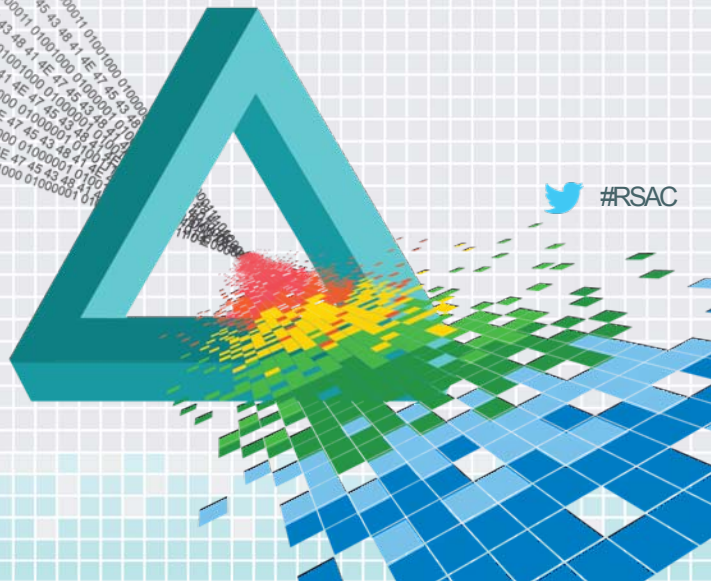
External attackers get all the press, but it's the insiders you need to worry about

- Current or former employees responsible for 66% of security incidents
- 84% of all attacks for financial gain are "non-technical"
- Vast majority of attacks involve compromised credentials
- 90% of data breaches were preventable
- More than 90% of security spend focused on perimeter protection

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Insider Risk Illustrated:
The Human Layer



Meet the Threats

PROFILE: Road Warrior

- Connecting remotely from all corners of the globe
- Mixes personal devices with business
- Circumvents security controls
- Saves everything (unencrypted) to the C: Drive of Personal MacBook
- Doesn’t report device theft for three weeks

Meet the Threats

PROFILE: Imperious Boss

- Wants 360-degree access to everything, 24/7
- Wants to use latest tech/devices/services
- Browbeats help desk into granting exceptions to policies
- Auto-forwards corporate email to personal Gmail account

UnitedLex

Meet the Threats

PROFILE: Careless Vendor

- Poor security controls
- Uses shared credentials to access your network
- Under-invested in security due to shrinking margins
- Answered your security questionnaire 5 years ago – no action since

UnitedLex

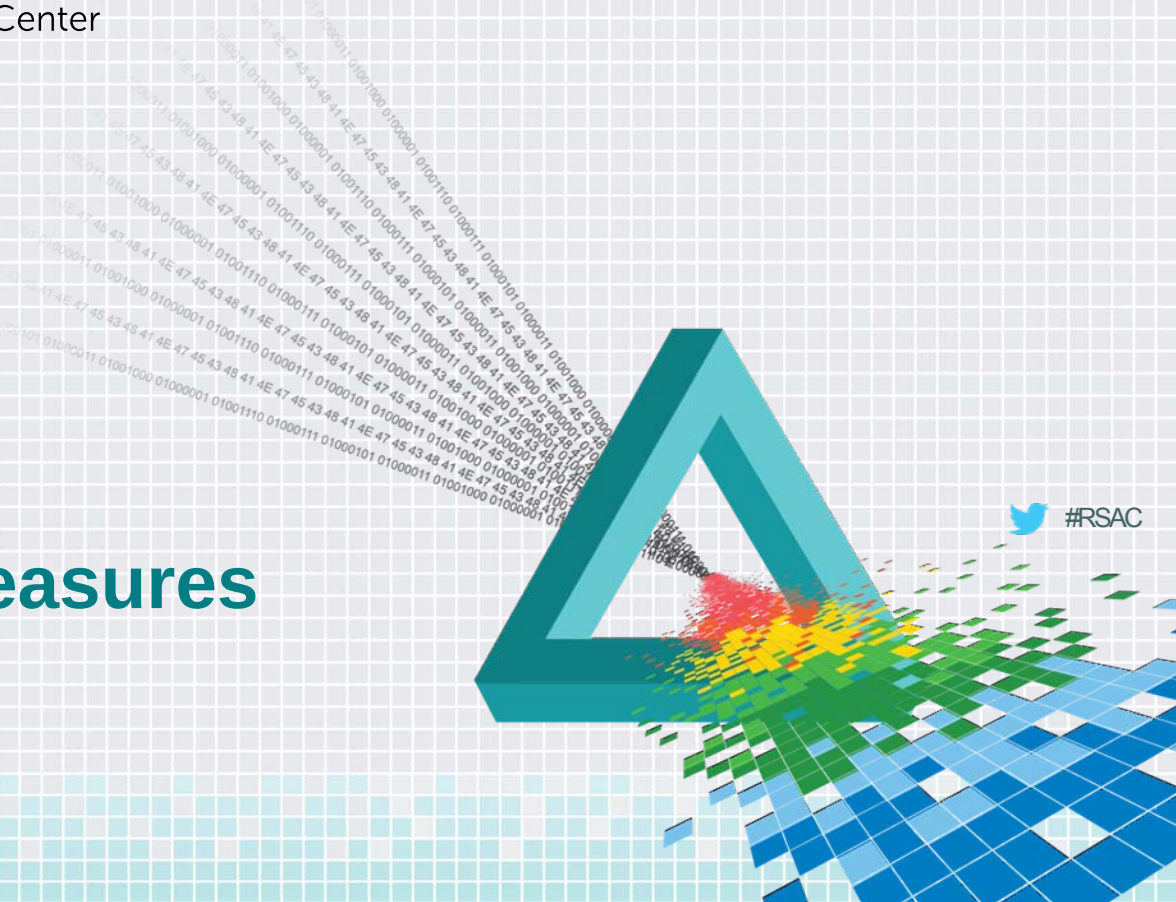
Meet the Threats

PROFILE: Disgruntled IT Manager

- File and email hoarder (just in case!)
- Passive saboteur
- Has keys to the IT kingdom
- Over-worked under paid
- Backdoor to boss's email box
- Backs up everything to DropBox (just in case!)

RSAConference2015

San Francisco | April 20-24 | Moscone Center



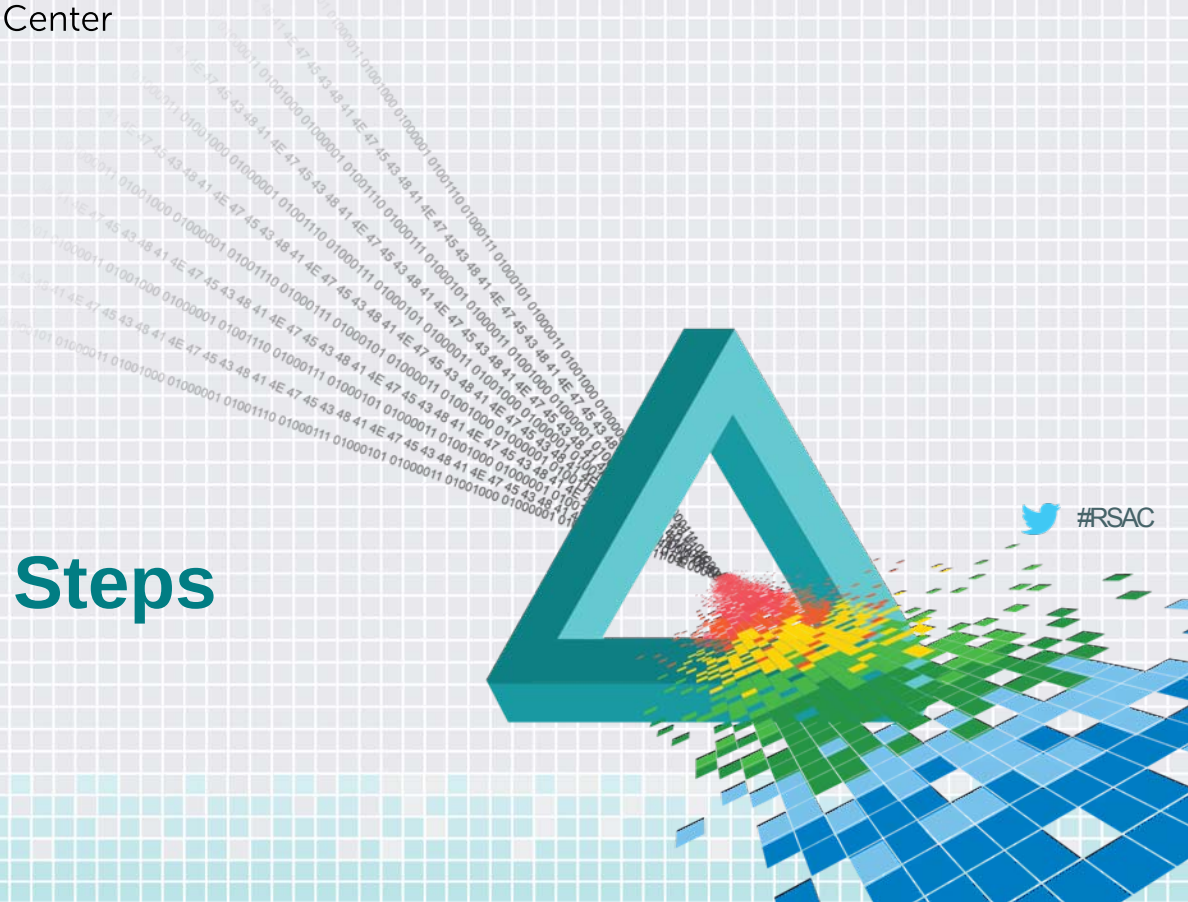
Risk Reduction Measures

How NOT to Address Insider Risks

- Create a police state that conveys you don't trust your employees
- Severely punish well-intended employees who make a mistake
- Impose disproportionate controls that impede effectiveness more than reduce risks
- BLINDLY BUY MORE TOOLS!

Simple Steps to Reduce Risk

1. Educate and engage senior executives in driving cultural change
2. Strictly limit number of privileged users and carefully consider segregation of duties
3. Transform vulnerabilities into fortifications through awareness training
4. Deploy intelligent behavioral monitoring technology to detect risky behavior by insiders (and vendors)
5. Implement and enforce clear, simple and DEFENSIBLE policies and controls



Conclusions/Next Steps

Apply What You Have Learned Today

- **Next week you should:**
  - Identify the key stakeholders needed to address insider threat risks
- **In the first three months following this presentation you should:**
  - Convene a meeting of key stakeholders to define a process to assess insider risks
  - Identify technology that could support your insider risk management program
- **Within six months you should:**
  - Have a roadmap for reducing and controlling insider risks
  - Implement an awareness program to introduce new insider risk measures

Resources

- Carnegie Mellon CERT Insider Threat Program: http://www.cert.org/insider-threat/
- FBI – Insider Threat Detection: http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat
- National Cybersecurity and Communications Integration Center: Combating the Insider Threat: https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf

RSAConference2015

San Francisco | April 20-24 | Moscone Center

QUESTIONS?

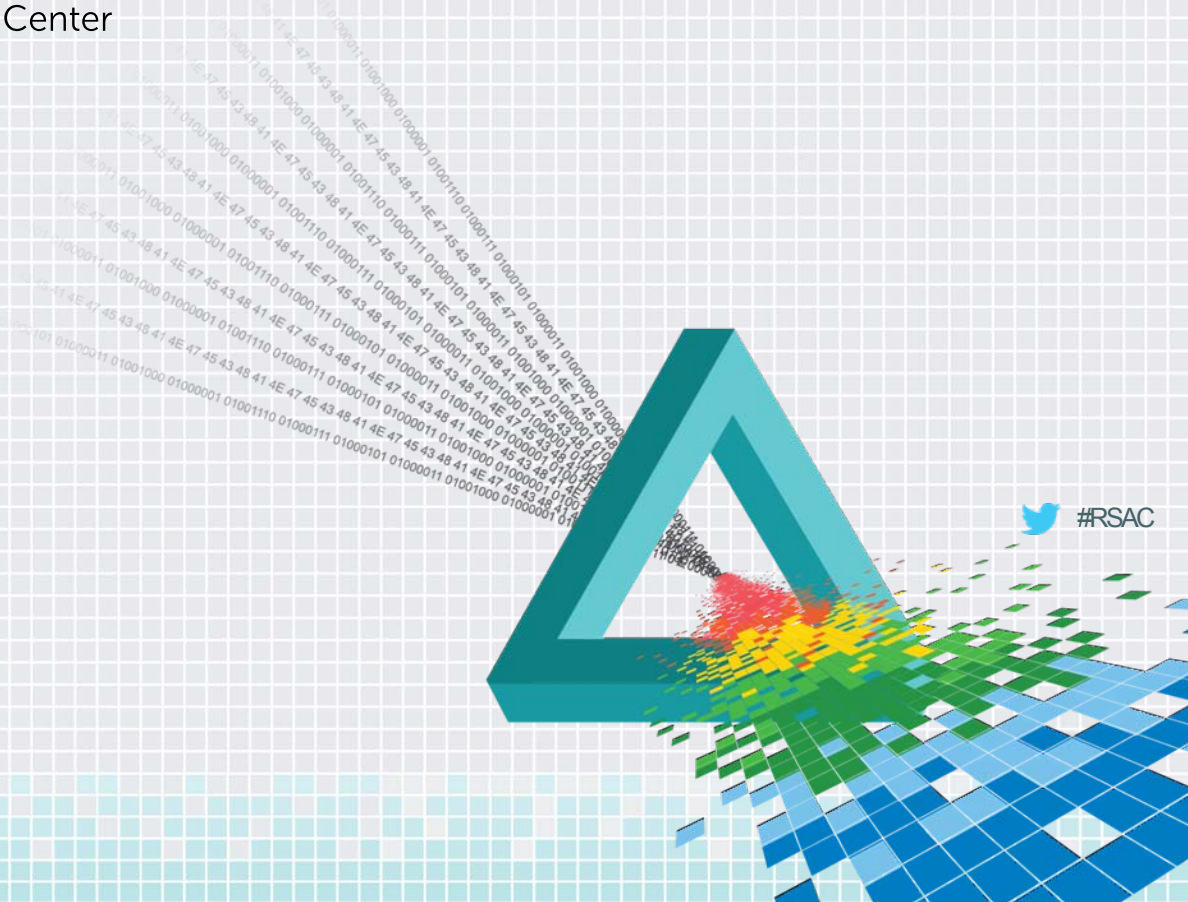
R Jason Straight

jason.straight@unitedlex.com

917-685-9504

RSAConference2015

San Francisco | April 20-24 | Moscone Center



Appendix

CERT Recommendations

1. Consider threats from insiders and business partners in enterprise-wide risk assessments
2. Clearly document and consistently enforce policies and controls (especially password and encryption policies)
3. Incorporate insider threat awareness into periodic security training for all employees.
4. Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.
5. Anticipate and manage negative issues in the work environment.
6. Know your assets.
7. Implement strict password and account management policies and practices.
8. Enforce separation of duties and least privilege.
9. Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
10. Institute stringent access controls and monitoring policies on privileged users.

CERT Recommendations

11. Institutionalize system change controls.
12. Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.
13. Monitor and control remote access from end points, including mobile devices.
14. Develop a comprehensive employee termination procedure.
15. Implement secure backup and recovery processes.
16. Develop a formalized insider threat program.
17. Establish a baseline of normal network device behavior.
18. Be especially vigilant regarding social media.
19. Close the doors to unauthorized data exfiltration.