Keep IT Simple, Stupid

Intro to IT Security

January 13, 2017

Nick DeLena, CISA, CRISC, MBA
Senior Manager

OCDTECH
A Division of O'Connor & Drew, P.C.

25 Braintree Hill Office Park, Suite 102, Braintree, MA 02184 • Phone: (617) 471-1120 • Fax: (617) 472-7560 • http://www.ocd-tech.com

SESSION GOALS

Understanding of:

- Concepts governing IT security
- Common threats
- Basic practices to secure our systems

Ground rules: ask questions anytime, keep me honest.

NICK DELENA

Senior Manager, IT Audit & Security

Nick DeLena, CISA, CRISC, is a Senior Manager at OCD Tech, the IT Audit & Security Division of O'Connor & Drew, P.C. Nick leads engagements across the division's primary practice areas, including audit, security, and advisory services. He's a 17-year veteran of IT and IT risk management, having audited, consulted, and managed IT teams in a variety of industries.

Education

- Brown University, Executive Masters in Business Administration
- Suffolk University, Sawyer School of Management, Bachelor of Science in Business Administration in Computer Information Systems, Minor in Finance

Certifications & Memberships

- Certified Information Systems Auditor (CISA), ISACA
- Certified in Risk and Information Systems Control (CRISC), ISACA
- Security+, CompTIA
- Information Technology Infrastructure Library Practitioner (ITIL)
- Member, InfraGard, a partnership between the private sector and FBI

OCDTECH

A Division of O'Connor & Drew, P.C.

ESTABLISHED 1949

HIGHLY COMPETENT: CISA CRISC CISSP C|EH

STANDARDS-DRIVEN: COBIT NIST SANS ISO

INDUSTRIES

- Financial Services
- Automobile Dealerships
- Real Estate
- Higher Education
- Not-for-Profit
- Government Entities

SERVICES

- IT Audit
- IT Vulnerability Assessments
- Physical Security Evaluation
- Penetration Testing
- Wi-Fi Vulnerability Assessment
- Confidential Data Review
- Backup Infrastructure Evaluation
- Firewall Testing
- End User Education
- Sarbanes Oxley 404 Testing
- FFIEC Cybersecurity Assessment
- Service Organization Control (SOC) Reports
- NIST Cybersecurity Framework Evaluations

INTRODUCTION

1 billion Yahoo accounts hacked

117 million LinkedIn accounts hacked

US accuses Russia of political cyberattacks

NSA hacking tools were stolen and auctioned

Hackers use DDoS attack to cut heat to apartment buildings

San Francisco MUNI hit with ransomware

CURRENT STATE OF CYBERSECURITY

MAJOR PROBLEM - THE SKILLS GAP

Pervasive lack of awareness in existing employee base ***and*** fewer graduates entering cybersecurity field.

- "Cybersecurity sector struggles to fill skills gap"
  Financial Times, November 18, 2015

- "Global shortage of **two million** cybersecurity professionals by 2017"
  UK Digital Skills Committee finding, 2014

- **30%** of data breaches the result of employee error
  Association of Corporate Counsel Survey, 2015

CURRENT STATE OF CYBERSECURITY

Security is critical, **but...**

It's too complex

Our staff isn't trained

The laws keep changing

We don't have enough resources

There are too few graduates with experience

Our executives don't get it

PRINCIPLES IN IT SECURITY

CIA Triad

PRINCIPLES IN IT SECURITY

PRINCIPLES IN IT SECURITY

Non-repudiation

The assurance that someone cannot deny something.

PRINCIPLES IN IT SECURITY

Principle of Least Privilege

Grant only the necessary permissions for an individual to do their job.

PRINCIPLES IN IT SECURITY

Encryption

Converting legible information into illegible code in such a way that only authorized parties can access it.

PRINCIPLES IN IT SECURITY

Defense-in-depth

The practice of layering controls to provide redundant protection for systems.

WHO ARE "HACKERS"?

HACKERS

Who are these "hackers"? A pretty diverse group…

- Script kiddies
- Hactivists
- White hat (ethical hackers, the "good guys")
- Gray hat
- Black hat

HACKER OBJECTIVES

VALUABLE INFORMATION

Objective of hacker is to find and exfiltrate valuable information, or hold your data hostage for $.

- Credit cards
- Social security numbers
- PII/PHI
- Intellectual property

HOW ARE THEY HACKING US?

ATTACK VECTORS

What are some successful attacks?

- Social engineering / phishing
- Password hacking
- Web application attacks
- Ransomware

OUR VULNERABILITY TO PHISHING

SOCIAL ENGINEERING

Psychological manipulation of people to perform a desired action.

23% of phishing recipients open message

11% click on attachments[1]

[1]Verizon's 2015 Data Breach Investigations Report

HOW BAD ARE WE AT PASSWORDS?

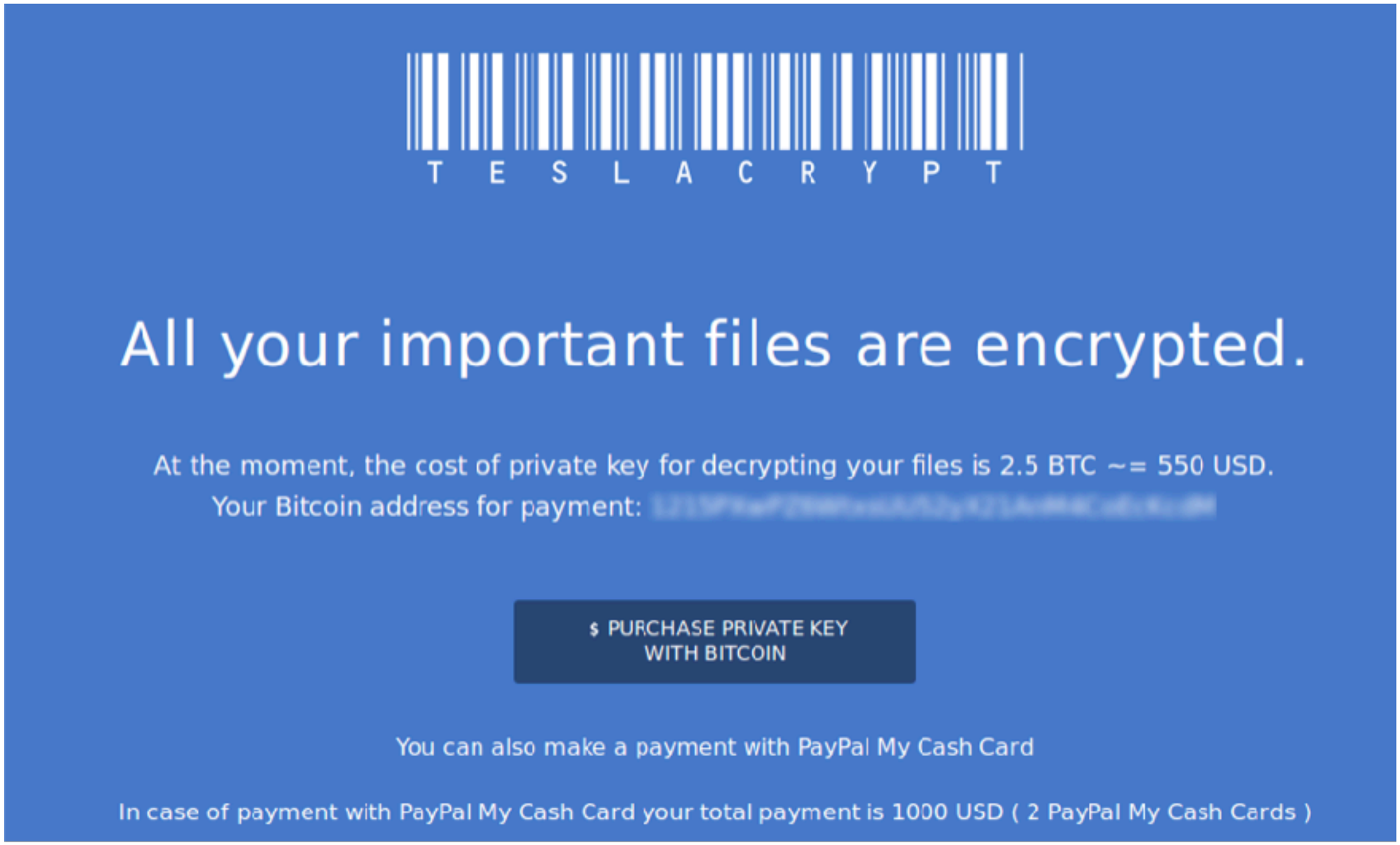
Really bad.

Top passwords from the LinkedIn Data Breach:

- 123456
- linkedin
- password
- 123456789
- 12345678
- 111111
- sunshine
- qwerty

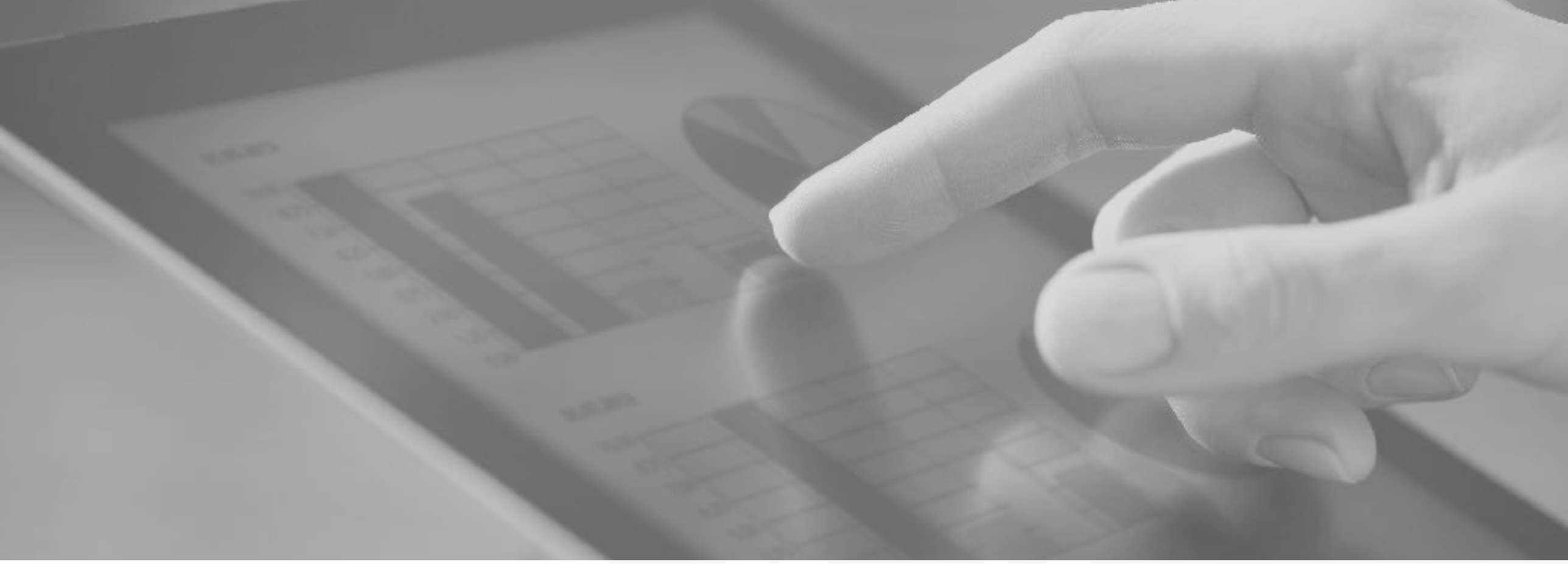
RANSOMWARE

ATTACK VECTORS



LIFECYCLE OF A HACK

ANATOMY OF A COMPROMISE



HOW CAN WE MITIGATE THE RISKS?

GOOD GOVERNANCE

DEFENSE

What can we do about it?

<u>First, check the laws & regs</u>

State data privacy laws

GLBA

FFIEC

GOOD GOVERNANCE

DEFENSE

What can we do about it?

Controls

Administrative, Technical, Physical

FFIEC IT Handbook

DEFENSE

What can we do about it?

Policies

Certain laws require them

Set tone + get top-level buy-in

DEFENSE

What can we do about it?

Staff Training

Conduct regular IT training for all staff

Test them regularly with phishing

Reward those that improve

DEFENSE

What can we do about it?

Patch Management

59% of successful computer hacks could have been prevented if the compromised computer was patched

Source: Solutionary, an NTT Group company

DEFENSE

What can we do about it?

Data Classification

Identify and protect your most important data.

GOOD GOVERNANCE

DEFENSE

What can we do about it?

<u>Third-party assessments</u>

Establish a baseline.

Where do you stand today?

NIST, SANS, CobiT, FFIEC CAT & ACAT

Thank You!

Questions?

Visit Us:

Booth 410

Amazon Echo raffle

OCDTECH

A DIVISION OF O'CONNOR & DREW, P.C.

25 Braintree Office Hill Park
Suite 102
Braintree, MA 02184

Telephone: (844) OCD-TECH

@TheOCDTech
@OCDCPA
http://www.ocd-tech.com
http://www.ocd.com

Find a copy of this presentation at:

http://ocd-tech.com/ocd-tech-at-bank-world/