Cybersecurity Threats in State Legislatures

Jeff Ford
Chief Technology/Security Officer
State of Indiana
Legislative Services Agency
Office of Technology Services

Certified Information Systems Security Professional (CISSP)
Global Information Assurance Certification (GSEC)

NALIT – Vice Chair

NALIT 2018 Cybersecurity Survey

- 25 states responded
- 48% use executive branch cybersecurity services
- 28% have a Chief Information Security Officer
- 26% have at least 1 dedicated Security Analyst
- 6 states use a security framework (NIST, ISO)
- 9 states provide security awareness training to legislators, but only 1 makes it mandatory
- 14 states provide security awareness training to legislative staff, but only 5 make it mandatory

Cybersecurity Threats in State Legislatures

"There's a war out there, old friend. A world war. And it's not about who's got the most bullets. It's about who controls the information. What we see and hear, how we work, what we think... it's all about the information! The world isn't run by weapons anymore, or energy, or money. It's run by little ones and zeroes, little bits of data. It's all just electrons (or photons ☺)"

--Cosmo, from Sneakers (1992)

10 Cybersecurity Truths

1. There is no 100% secure, only varying degrees of security
2. The most secure systems are the best managed systems
3. All good security is custom fit– compliance does not equal security
4. When security gets in the way of the mission—security is wrong, not the mission
5. You can't secure what you can't control
6. You can't prevent what you allow
7. Prevention is ideal, detection is a must, detection without response is useless

Securing our Infrastructure

Legislative Services Agency
Office of Technology Services

Securing our Devices

AI and Machine Learning in Cybersecurity

- The need for a cybersecurity overhaul is necessary as the traditional practices are no longer effective in identifying and preventing attacks
- The growing capabilities of artificial intelligence are triggering a battle across the cyber security fence – and organizations must act now to be on the right side of it
- Recognize what machines do best and what people do best
- Use AI to do the repetitive work and look for anomalies
- AI acts as the inference engine that feeds the cybersecurity decision makers
- AI will keep us, the defenders, ahead of the adversary, the attackers

AI and Machine Tools

CROWDSTRIKE

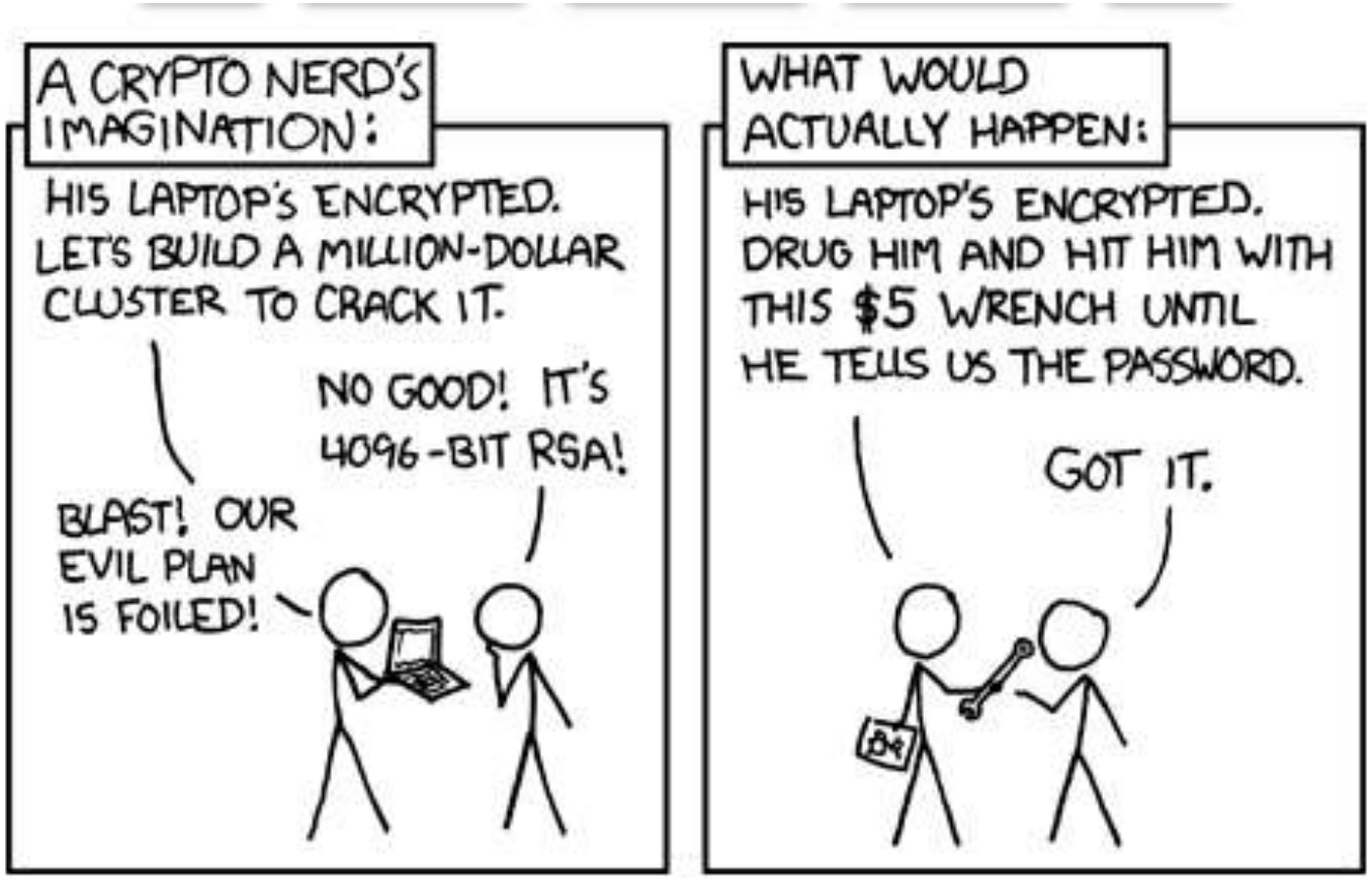
RAPID7

ExtraHop

CLOUDFLARE

CYLANCE

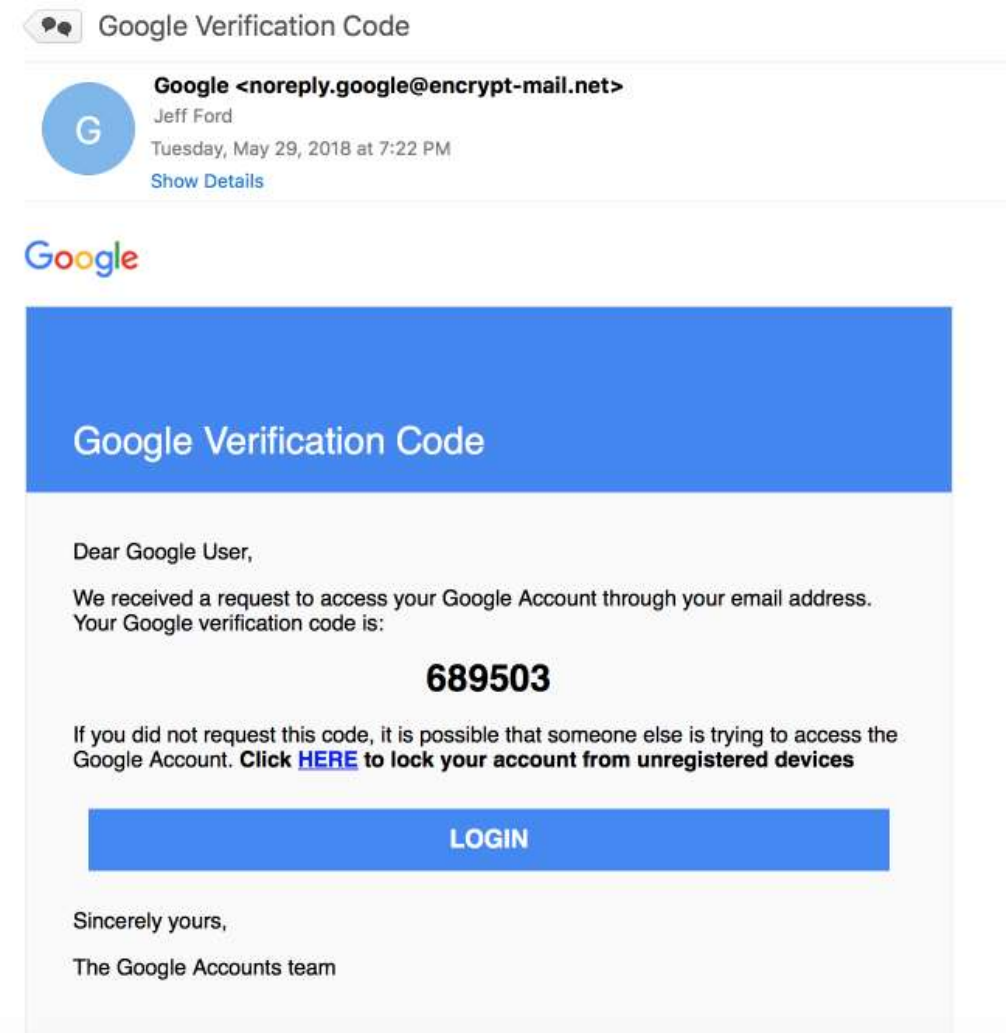
8. You cannot process encrypted data… EVER



Types of Hackers

- Organized Crime
- Nation State
  - **Advanced Persistent Threat (APT)**
- **Script Kiddies**
- **Hacktivists**
- **Insiders**

Phishing


Google Verification Code
Google <noreply.google@encrypt-mail.net>
Jeff Ford
Tuesday, May 29, 2018 at 7:22 PM
Show Details
Google
Google Verification Code
Dear Google User,
We received a request to access your Google Account through your email address.
Your Google verification code is:
689503
If you did not request this code, it is possible that someone else is trying to access the Google Account. Click HERE to lock your account from unregistered devices
LOGIN
Sincerely yours,
The Google Accounts team

Social Engineering

Spear Phishing

To: Jeff Ford (jeff.ford@iga.in.gov)
From: Geoff DePriest (geoff.depriest@iga.in.gov)

Subject: Budget Meeting Follow-up

Please review the notes from our budget meeting this morning. Make sure track changes are on and return it to me when you are done.

Thanks,

Geoff

Attachment: 2018budget_v2

10 Cybersecurity Truths

9. Security is, first and foremost, a people issue
10. The most dangerous thing in the world is what you think you know

Why security awareness?

- 87% of all breaches happened in minutes or seconds and 68% went undiscovered for months
- The majority of all breaches are found by non-IT staff
- Humans, just like other operating systems, have vulnerabilities, but they are psychological ones, not technical ones
- Humans overestimate risk for highly visual events and for events in which they are not in control

Things to Remember

- We don’t operate inside of castles anymore, protect your endpoints
- Our most valuable security assets are our employees
- Security can no longer be just part of someone's job description

Resources

- MSISAC – Multi-State Information Sharing and Analysis Center
- US-CERT – United States Computer Emergency Readiness Team
- http://www.newsnow.co.uk/h/Technology/Security
- Hacker News
- Brian Krebs
- John Strand – Black Hills Information Security
- Bryce Galbraith – SANS Institute

Contact Information

Jeff Ford
Chief Technology/Security Officer
State of Indiana
Legislative Services Agency
Office of Technology Services

jeff.ford@iga.in.gov
Twitter: @jeffridford