TROY UNIVERSITY

Common Cyber Security Myths
An Update on Cyber Security

During the last minute…

45 new viruses emerged

200 new malicious websites launched

180 identities stolen

5,000 new versions of malware created

$2,000,000 lost

Prevalence of Cybersecurity Issues

- 2016 – Almost 80,000 documented incidents and 2,100+ confirmed data breaches
- Ten vulnerabilities accounted for 97% of all documented exploits
- The remaining 3% consist of over 7,000,000 different vulnerabilities, some dating to 1999
- Average cost per stolen record: $213.00
- Since 2005, 4,500+ data breaches have been announced
- Average breach time is less than two minutes
- 23% response to Phishing attempts

Cybersecurity Trends

- Specificity of targets have increased since 2005
  - Casting a wider net, with a directed approach
- Users continue to be a major source of problems
  - 73% of successful attacks are attributed to user problems
  - 42% of successful attacks result from misconfigured systems
  - 31% of successful attacks result from end-user error
- Poor security awareness and IT product management
  - 99.9% of the exploited vulnerabilities in 2016 had associated patches that were over 1 year old
  - Awareness campaigns are often poorly designed and lack “teeth”
- 96% of mobile malware targets Android devices

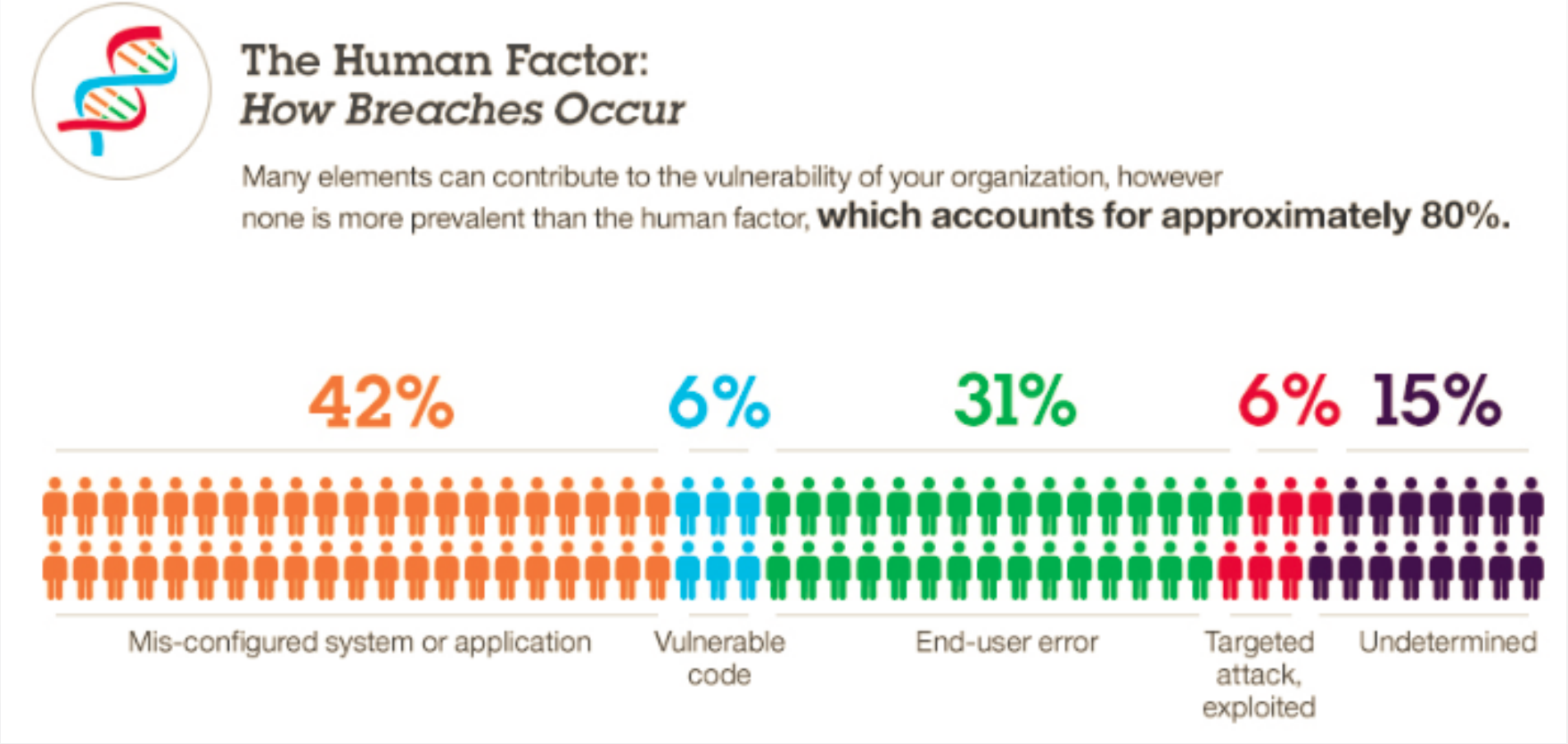
Attacks and Incidents

Myth #1 – It Won't Happen to Me!

- Common misconception
- Small doesn't mean overlooked
- We don't store anything significant
- All of my stuff is stored in "the cloud"
- My wife's cousin's son is really smart

Small businesses suffer the majority of attacks – However, colleges remain a prime target

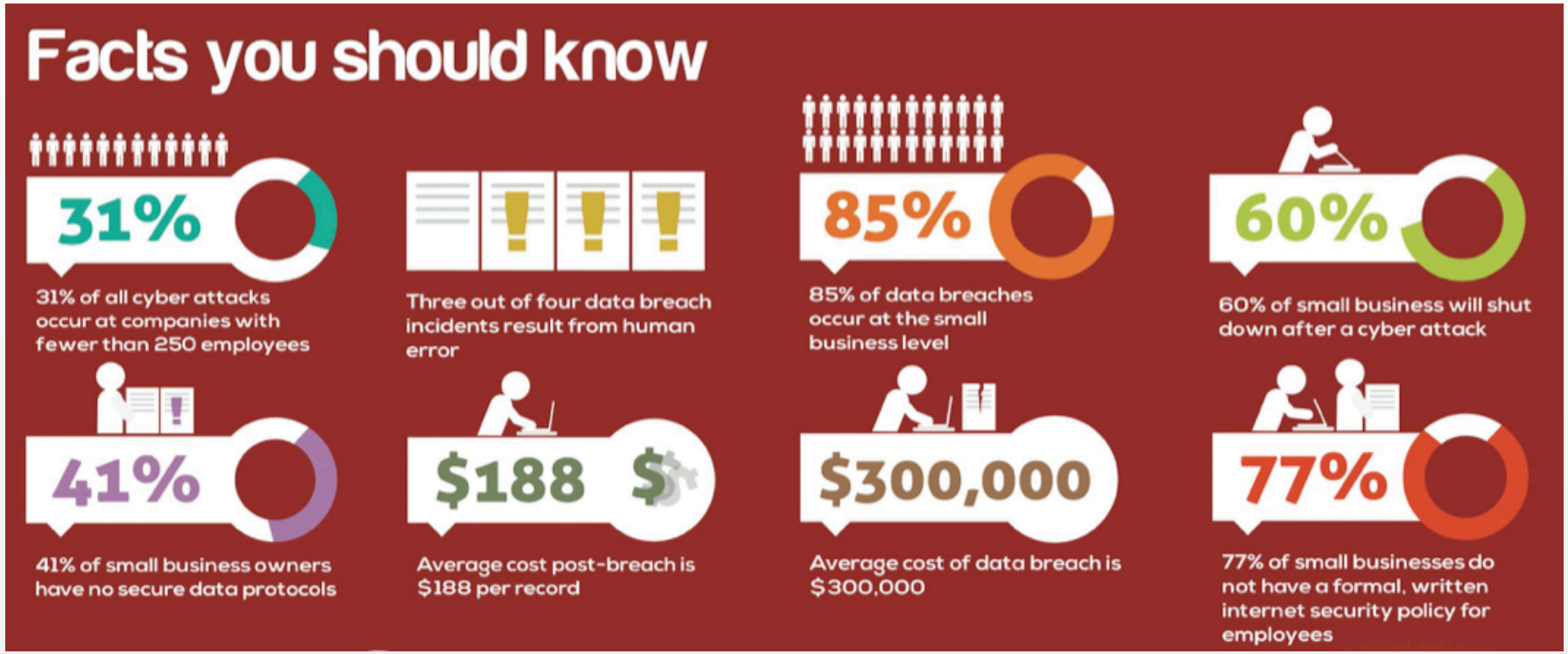
They are already in…



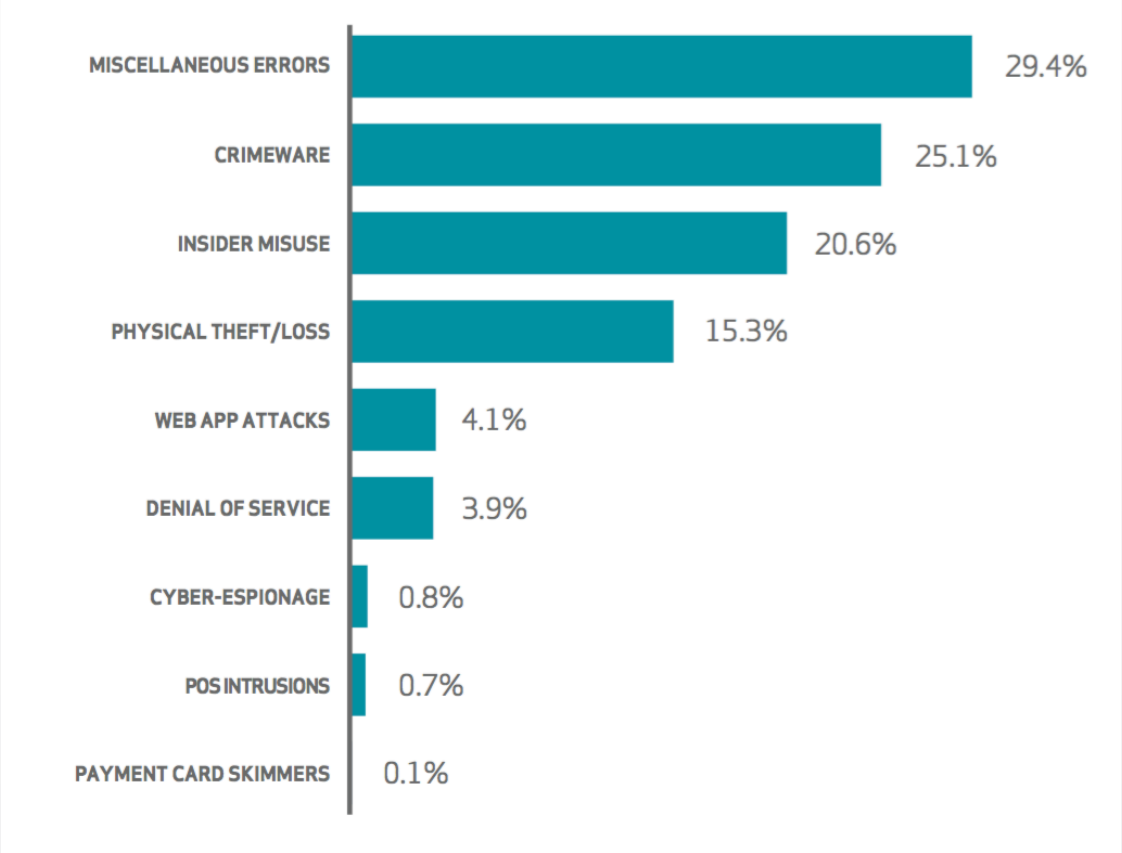
TROY UNIVERSITY

it.troy.edu/security

Cybersecurity Trends – Small Businesses, Colleges



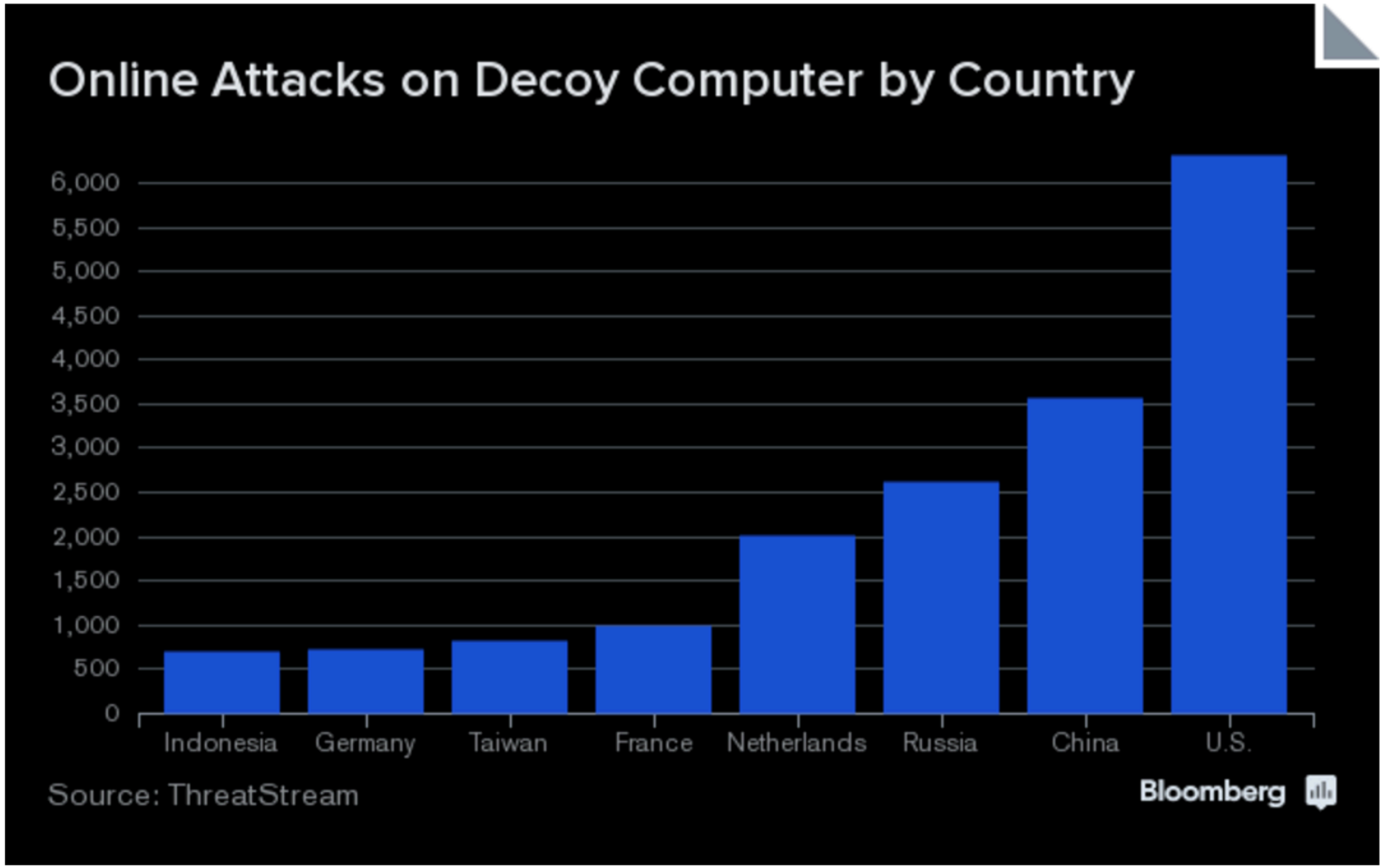
Myth #2 – Hackers are geniuses from over there…



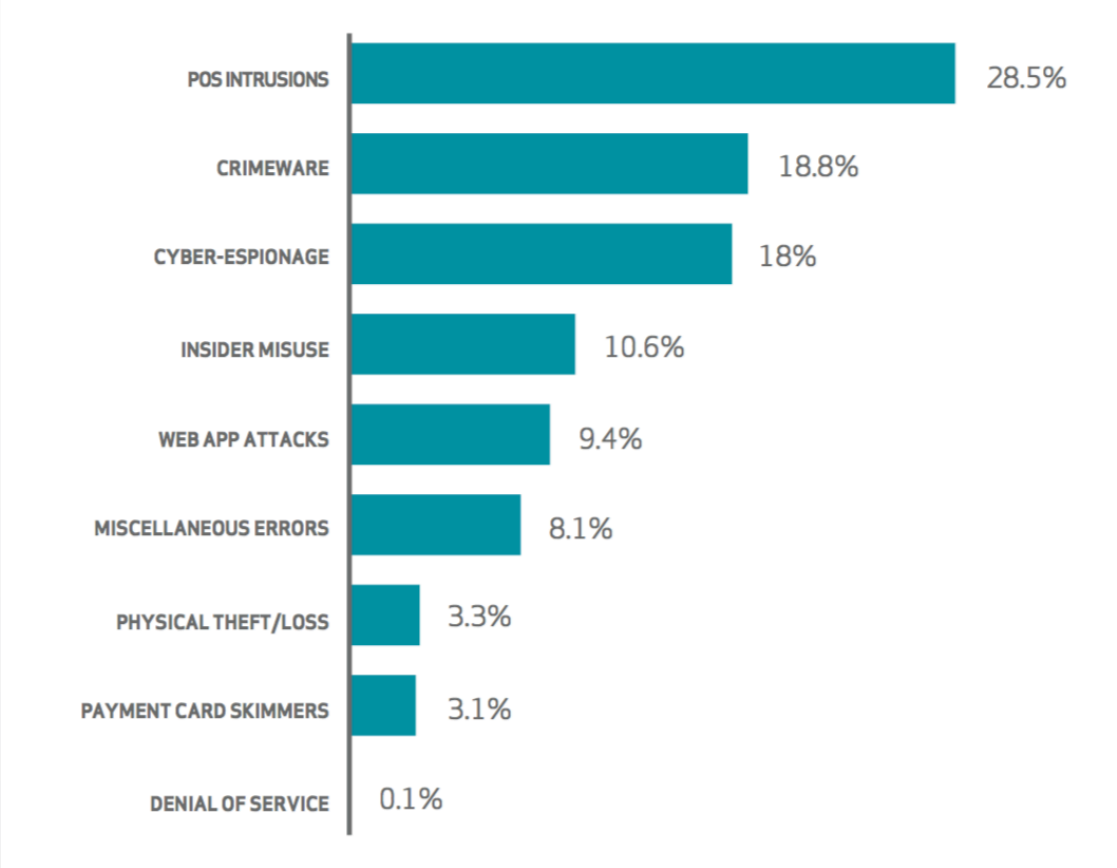
Myth #2 – Hackers are geniuses from over there…

Top Ten Hacking Countries

1.	China	41 percent (of the world's attack traffic)
2.	U.S.	10 percent
3.	Turkey	4.7 percent
4.	Russia	4.3 percent
5.	Taiwan	3.7 percent
6.	Brazil	3.3 percent
7.	Romania	2.8 percent
8.	India	2.3 percent
9.	Italy	1.6 percent
10.	Hungary	1.4 percent



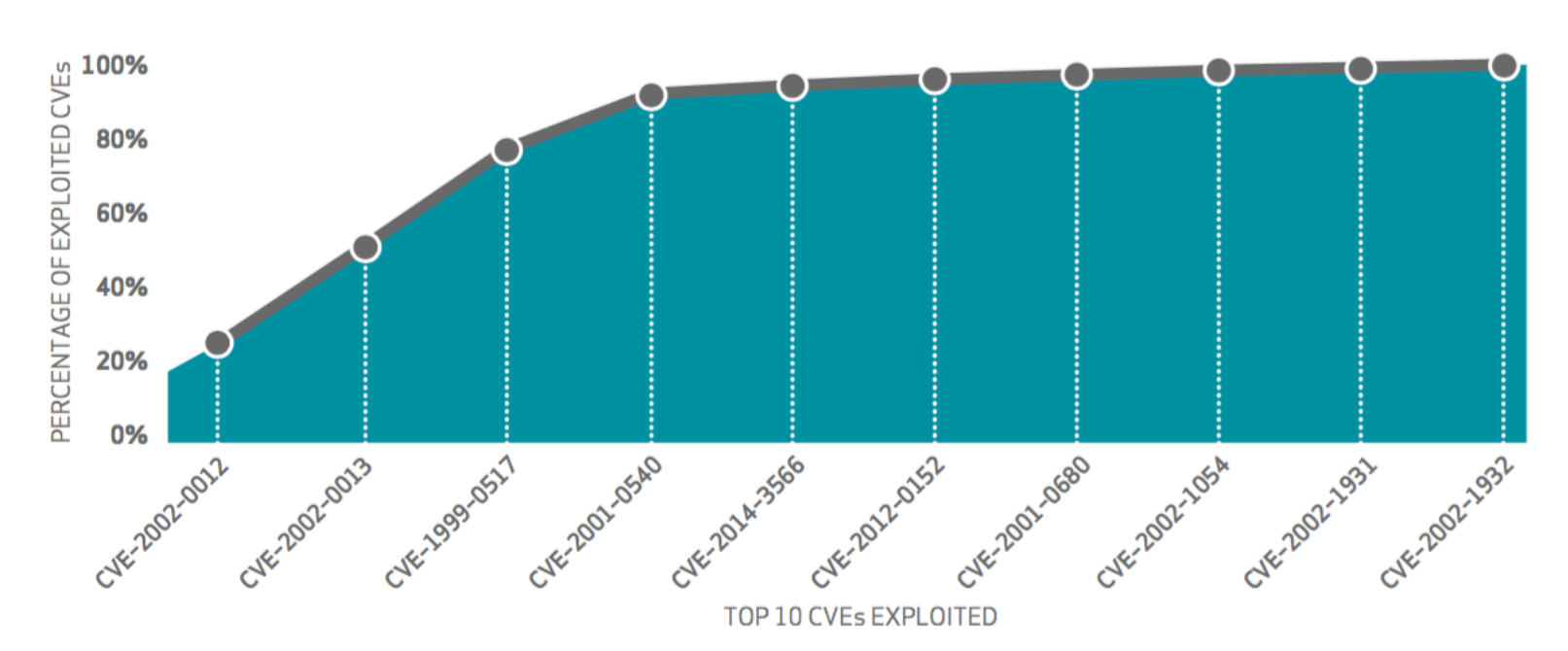
Myth #3 – "But I bought that thingy…"



“Are you sure?”

99.9%

OF THE EXPLOITED VULNERABILITIES WERE COMPROMISED MORE THAN A YEAR AFTER THE CVE WAS PUBLISHED.



Attacks and Incidents

2 **Most Common Attacks**

The two most common types of attacks combined account for **over 60% of all incidents.**

35%

MALICIOUS CODE

A term used to describe software created for malicious use. It is usually designed to disrupt systems, gain unauthorized access, or gather information about the system or user being attacked.

Third party software, Trojan software, keyloggers, and droppers can fall into this category.

28%

SUSTAINED PROBE / SCAN

Reconnaissance activity usually designed to gather information about the targeted systems such as operating systems, open ports, and running services.

What's Hot?

- Social Engineering – Phishing, Spear-Phishing
- Wifi Hijacking
- Side-Jacking
- Ransomware
- Poor patching practices
- Close loop on poor HR processes – know who's in, and who shouldn't
- Regulatory – FERPA, PCI, GLBA, HIPAA, EUGDPR, NIST 800

HOW DATA BREACHES ENROLL AT UNIVERSITIES

1. **Malware and viruses**
   Malware and viruses enter a university's systems with malicious intent or by accident. Either way, once in a university's system, malware and viruses go to work deleting files and stealing passwords, bank accounts and other sensitive information.

2. **Unsafe software and apps**
   Similar to malware and viruses, unsafe software and apps that are downloaded onto systems or devices open the floodgates for personal information to be shared with the world or cause hardware to completely shut down.

3. **Personal services downloads**
   Most, if not all, faculty and staff at a university utilize personal email accounts and services such as Dropbox on their devices. While Dropbox in itself is not a harmful service, when personal services are downloaded and used outside of a university's scope, these seemingly safe services can be a vessel for data breaches. Unprotected services are subject to attack and often go unnoticed because IT is unaware that these services are being run on institutionally owned hardware.

4. **Unsafe network practices**
   With today's workforce as mobile as ever, it's very common for faculty and staff to connect to their university's network from home or a coffee shop. If users are not utilizing the university's secure virtual private network (VPN), they can inadvertently leave the network vulnerable to attack.

5. **Unencrypted devices**
   Faculty and staff are not immune to mistakes and can forget their device or a USB stick on or off campus. When devices are lost—or stolen—they are prime targets for data breaches.

Five major areas of concern

How?

- Patch Management – Secunia, SCCM, WSUS
- Whitelisting, Remove local admin
- Better A/V – Cylance, Carbon Black
- SIEM – Splunk, Alien Vault, Qradar, OpenSource
- Security Response Team
- External Audits
- Close the HR loop
- NAC with onboarding
- Encryption – MBAM
- Lateral Movement – exfiltration – watch the logs - CnC
- Recursive DNS – create blackhole routing paths
- Mandatory password expiration – REACT, NO! Complex
- Network Segmentation, no, Segregation – VPN internally
- Mandatory Security Training – Secure the Human – SANS
- Phishing – phish yourselves, Phish.Me, Metasploit

Ransomware

1. Are you training users on the dangers of phishing?
2. Do you back up your business data regularly?
3. Do you have anti-phishing email security?
4. Have you deployed endpoint security with specific ransomware protection?
5. Are your mobile devices secure?
6. Do you have a patch management policy?

In the media…

https://campustechnology.com/articles/2017/01/10/community-college-pays-hacker-2

Community College Pays Hacker $28,000 for Ransomware Attack

By Staff | 01/10/17

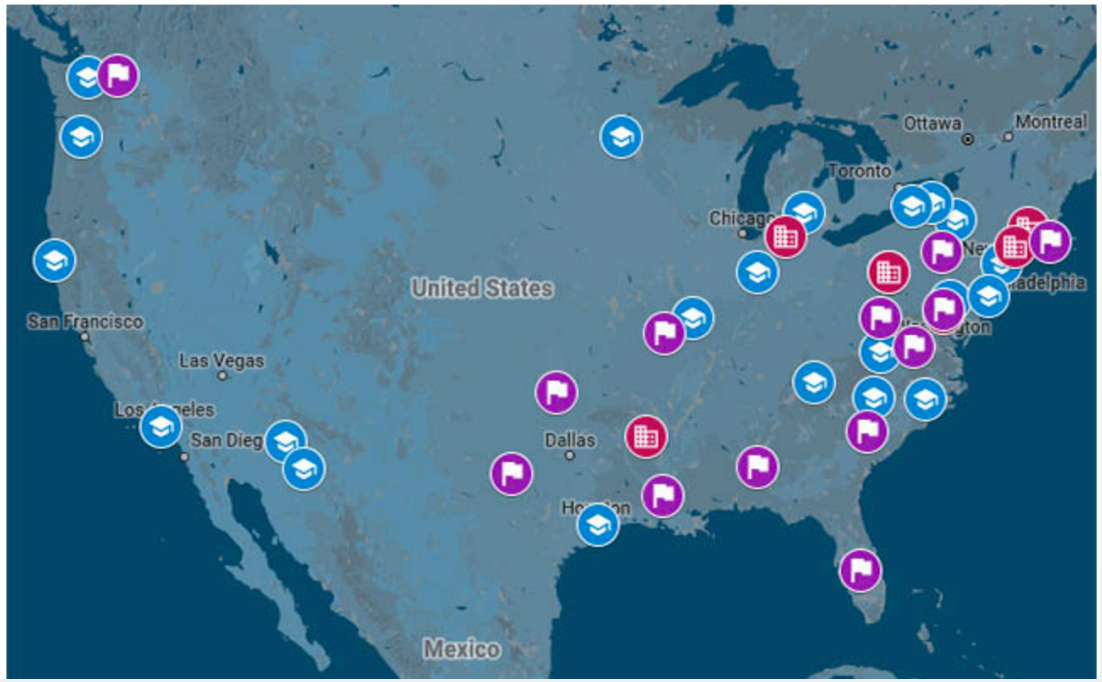
Last month, Los Angeles Valley College (LAVC) was hit with a ransomware attack, forcing the California Community College system to pay an unidentified hacker nearly $28,000 to retrieve stolen data. The investigation is still in the early stages, and as of now no breach data was identified.

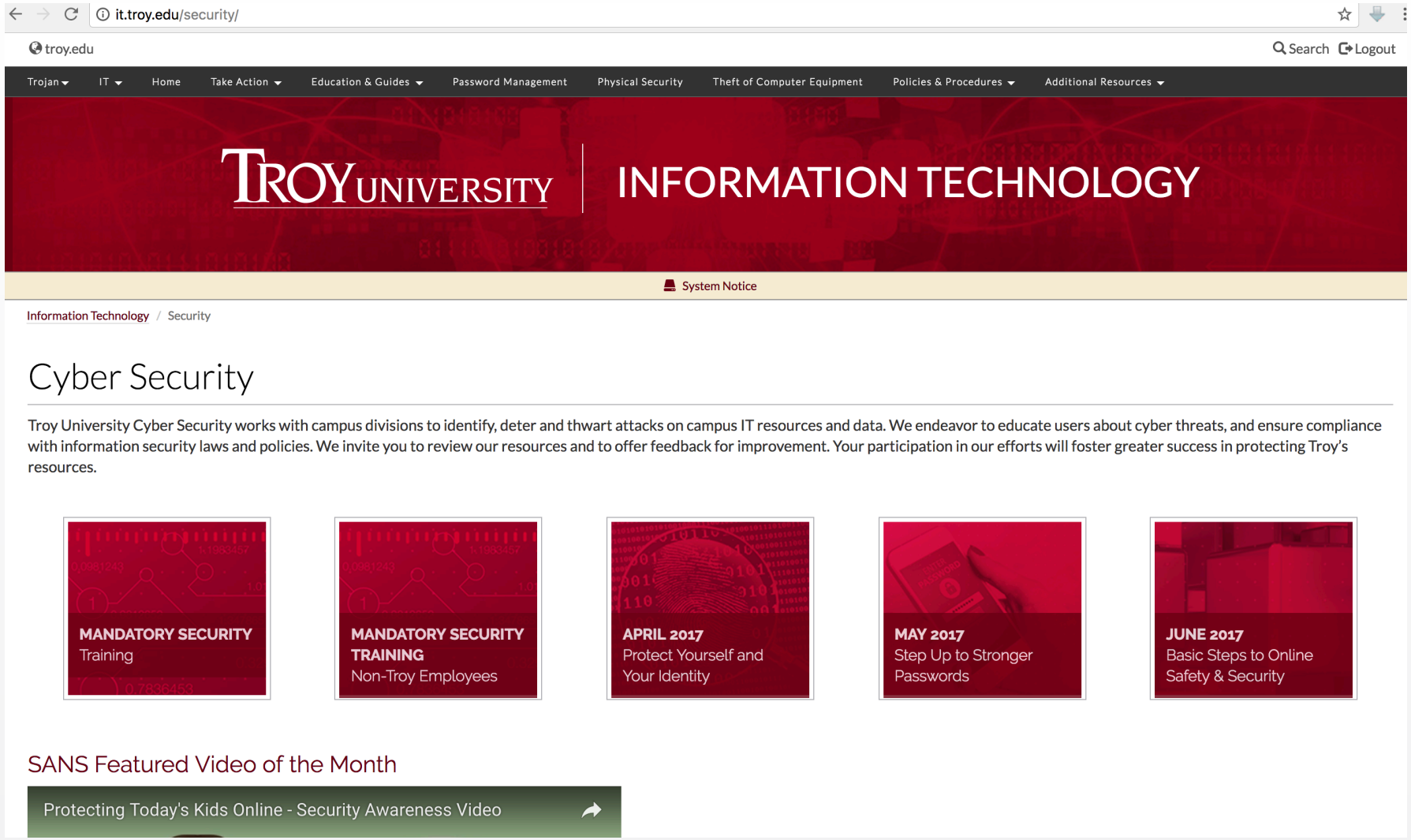
LAVC consulted with its leadership, outside cybersecurity experts and law enforcement before making the payment. "It was the assessment of our outside cybersecurity experts that making a payment would offer an extremely high probability of restoring access to the affected systems, while failure to pay would virtually guarantee that data would be lost," according to a statement. The attack

Security

'Rasputin' Hacker Targets 60 Universities, Government Agencies

By Sri Ravipati | 02/21/17





W. Greg Price, PhD

wgprice@troy.edu