Protecting Campuses from Data Breach

Diane McCracken, EVP, Chief Security Officer - BankMobile

Ray Parris, Vice President of Sales – BankMobile

Moderator: Kashu Vyas, District Director of Fiscal Affairs - North Orange County CCD

BankMobile

Who is BankMobile?

- Offers Refund Management®
- More than 200 staff members, headquartered in New Haven, CT
- Nearly 5 million students receive their disbursements from BankMobile
- BankMobile delivers 1 out of 3 student refunds in the United States

18

years of
Refund Management

approximately

800

campuses served

over

1.8M

account holders

Who Am I?

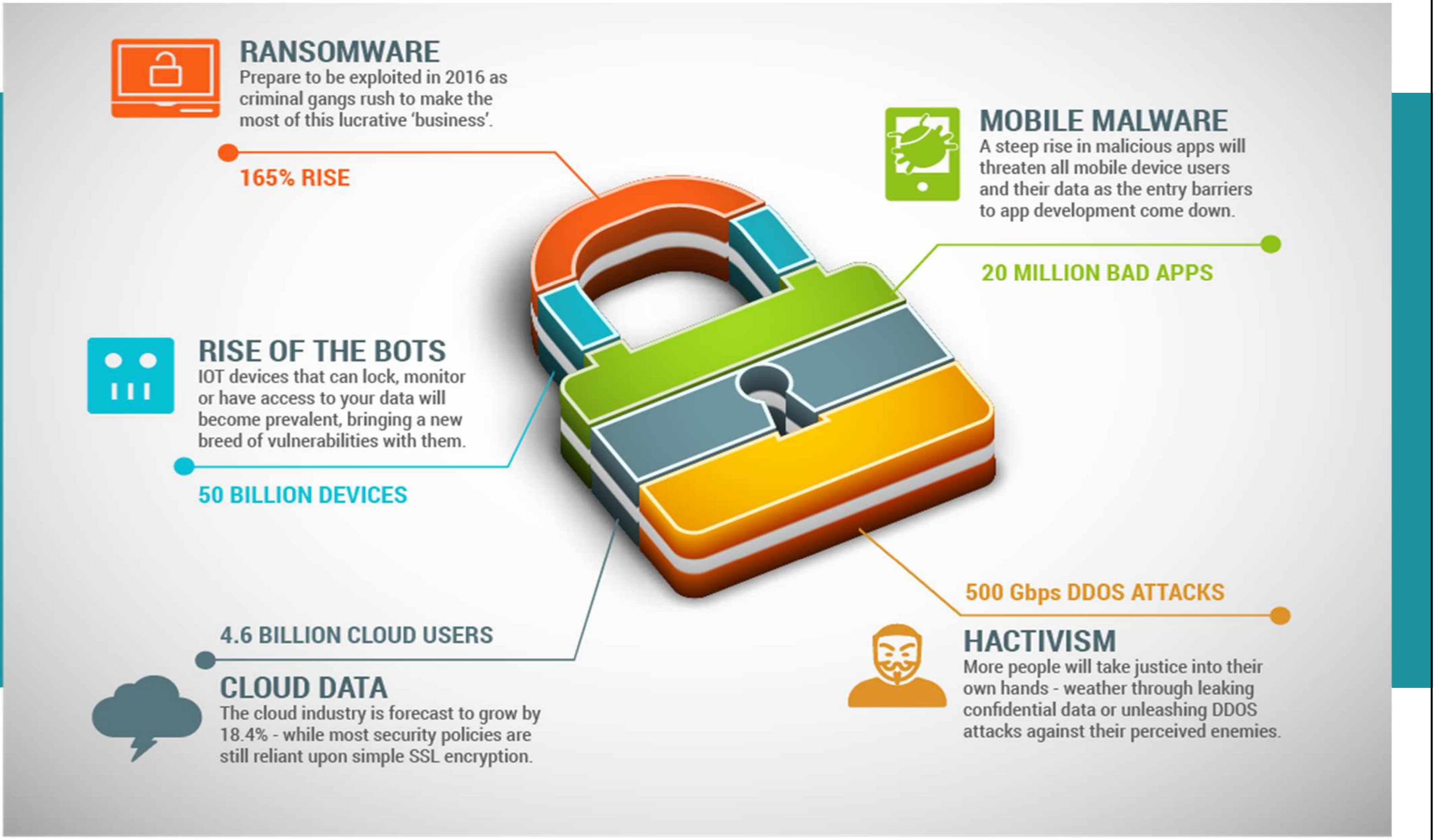
- Certified Information Systems Security Professional (CISSP)
- Technologist
- Business-enabler
- Cybervangelist
- Member of ISC2, ISSA, FS-ISAC, BankInfoSecurity, InfraGard, ACP

Today

1) Cybercrime environment
2) Who are the targets?
3) Why do they do it?
4) How are they attacking?
5) What's the cost?
6) What can higher education professionals be doing?

Organizations lost $301 per employee due to endpoint attacks in 2017

Cyber Security Trends



RANSOMWARE

Prepare to be exploited in 2016 as criminal gangs rush to make the most of this lucrative 'business'.

165% RISE

MOBILE MALWARE

A steep rise in malicious apps will threaten all mobile device users and their data as the entry barriers to app development come down.

20 MILLION BAD APPS

RISE OF THE BOTS

IOT devices that can lock, monitor or have access to your data will become prevalent, bringing a new breed of vulnerabilities with them.

50 BILLION DEVICES

500 Gbps DDOS ATTACKS

HACTIVISM

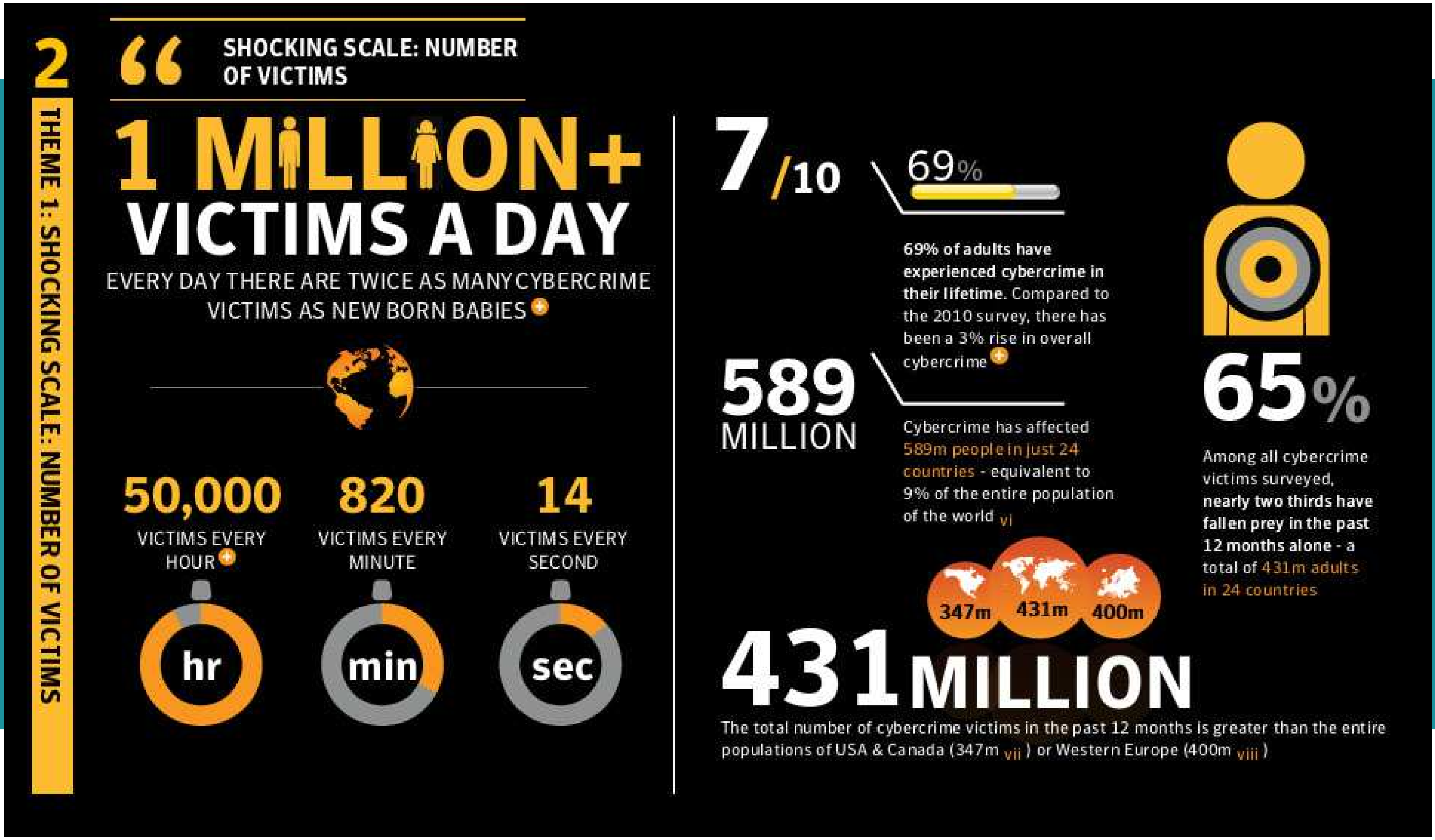
More people will take justice into their own hands - weather through leaking confidential data or unleashing DDOS attacks against their perceived enemies.

4.6 BILLION CLOUD USERS

CLOUD DATA

The cloud industry is forecast to grow by 18.4% - while most security policies are still reliant upon simple SSL encryption.

Who is a Target?



2 “ SHOCKING SCALE: NUMBER OF VICTIMS

THEME 1: SHOCKING SCALE: NUMBER OF VICTIMS

1 MILLION+ VICTIMS A DAY

EVERY DAY THERE ARE TWICE AS MANY CYBERCRIME VICTIMS AS NEW BORN BABIES

50,000 VICTIMS EVERY HOUR

820 VICTIMS EVERY MINUTE

14 VICTIMS EVERY SECOND

7/10

69%

69% of adults have experienced cybercrime in their lifetime. Compared to the 2010 survey, there has been a 3% rise in overall cybercrime

589 MILLION

Cybercrime has affected 589m people in just 24 countries - equivalent to 9% of the entire population of the world vi

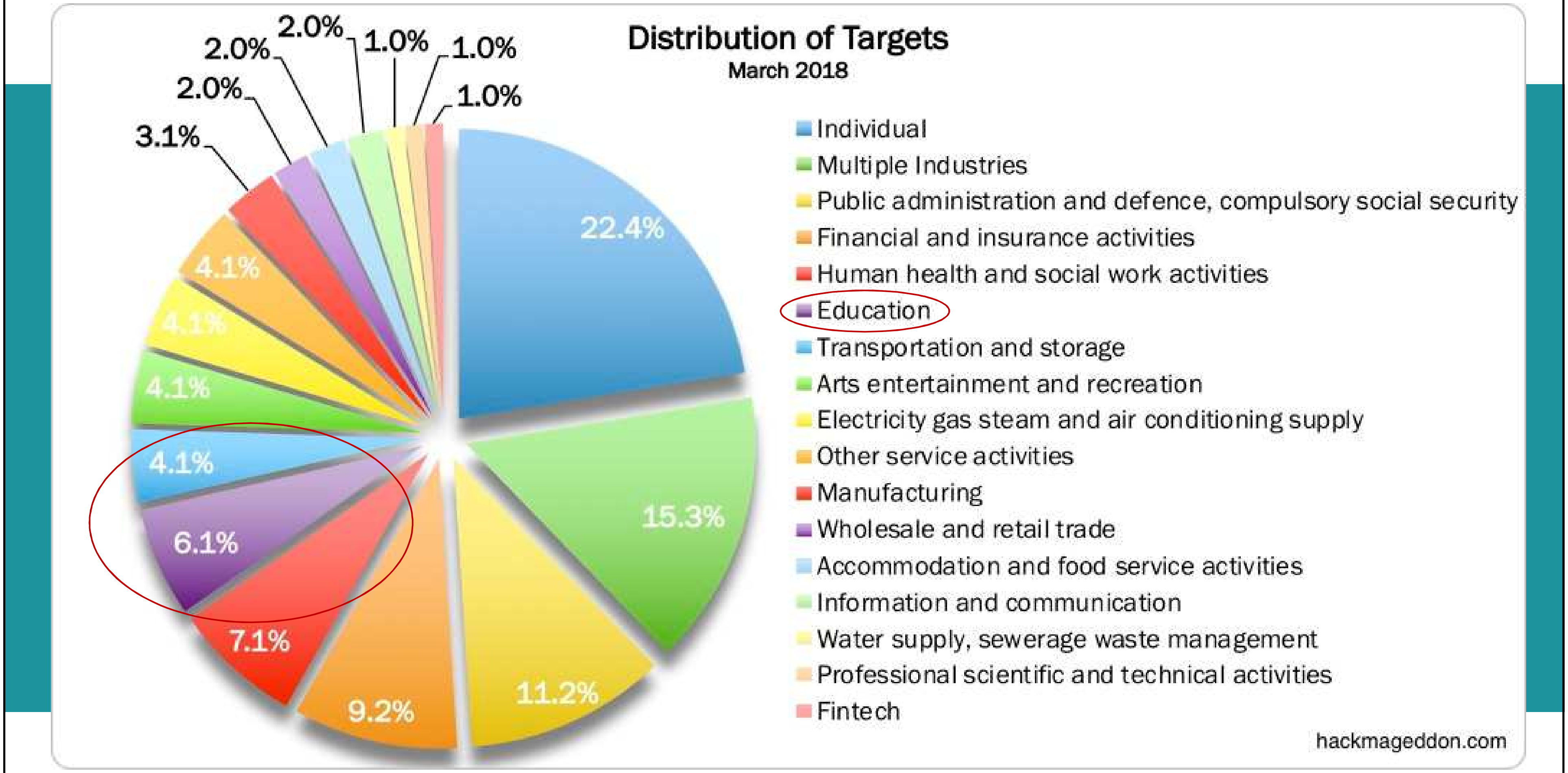
65%

Among all cybercrime victims surveyed, **nearly two thirds have fallen prey in the past 12 months alone** - a total of 431m adults in 24 countries

431 MILLION

The total number of cybercrime victims in the past 12 months is greater than the entire populations of USA & Canada (347m vii) or Western Europe (400m viii)

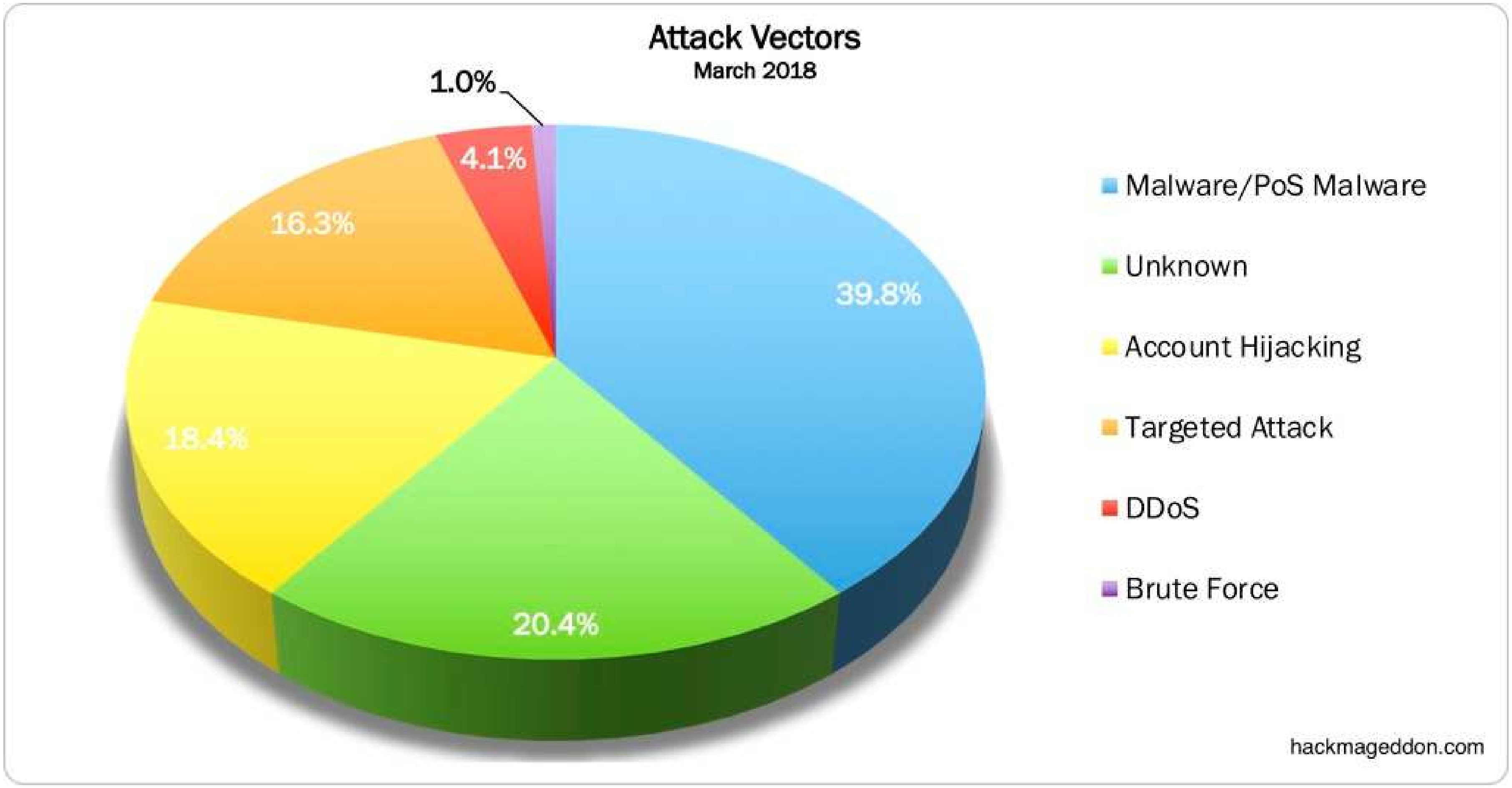
Who is a Target?



Why is Higher Education a Target?

- Social Security numbers, bank accounts, credit cards, health information and students' parents' information are hot items for hackers
- Breaches at universities were up 164% in the first 6 months of 2017
- Securing data poses an enormous challenge as the cycle of students, alumni, and faculty constantly changes
- Universities and colleges can have multiple networks and systems that are difficult to integrate
- In-house programs could have been developed years ago and are now outdated, making them difficult to modify and upgrade and difficult to secure

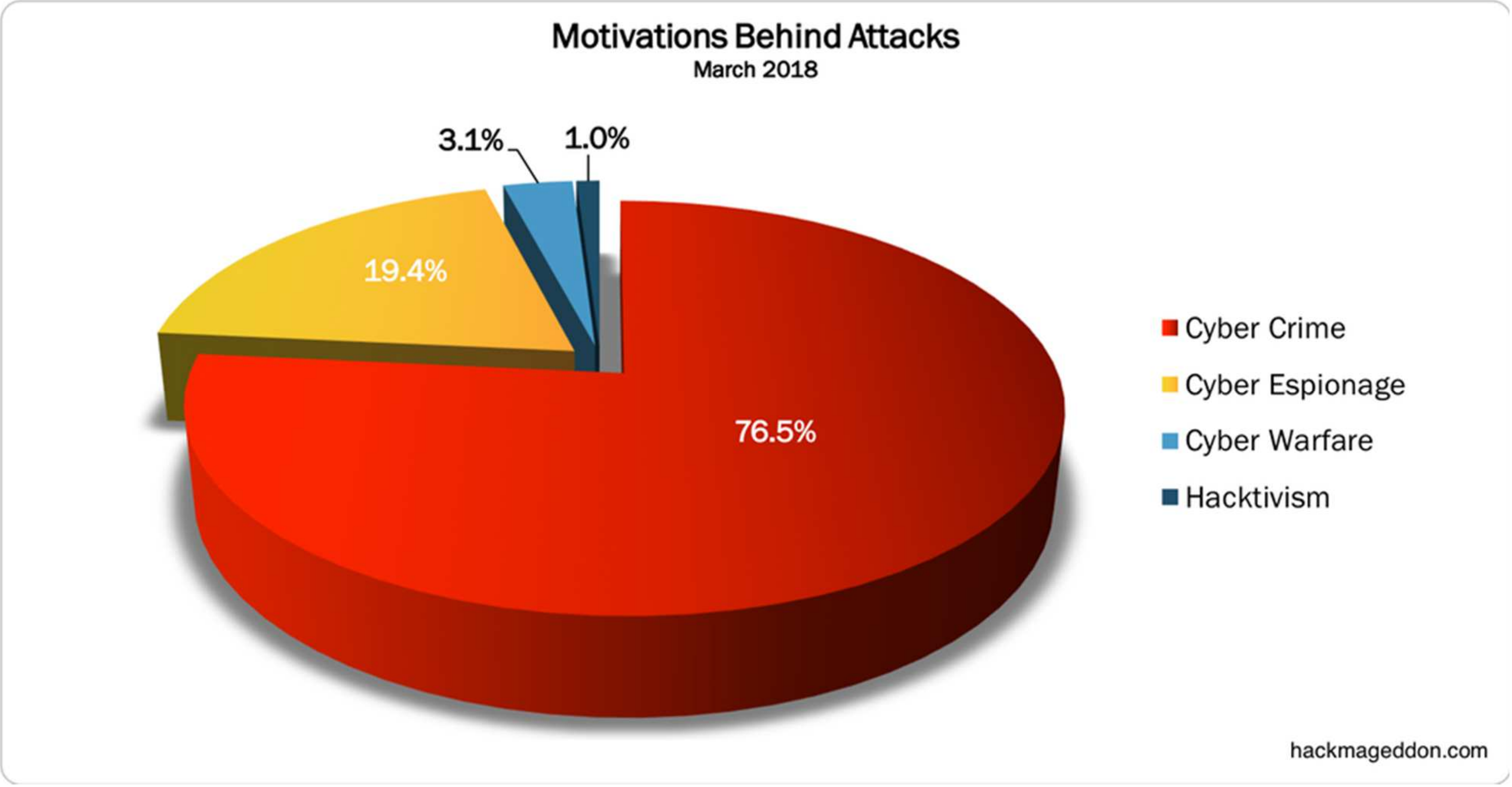
How Are They Attacking?



Attack Vectors
March 2018

hackmageddon.com

Why Do They Do It?



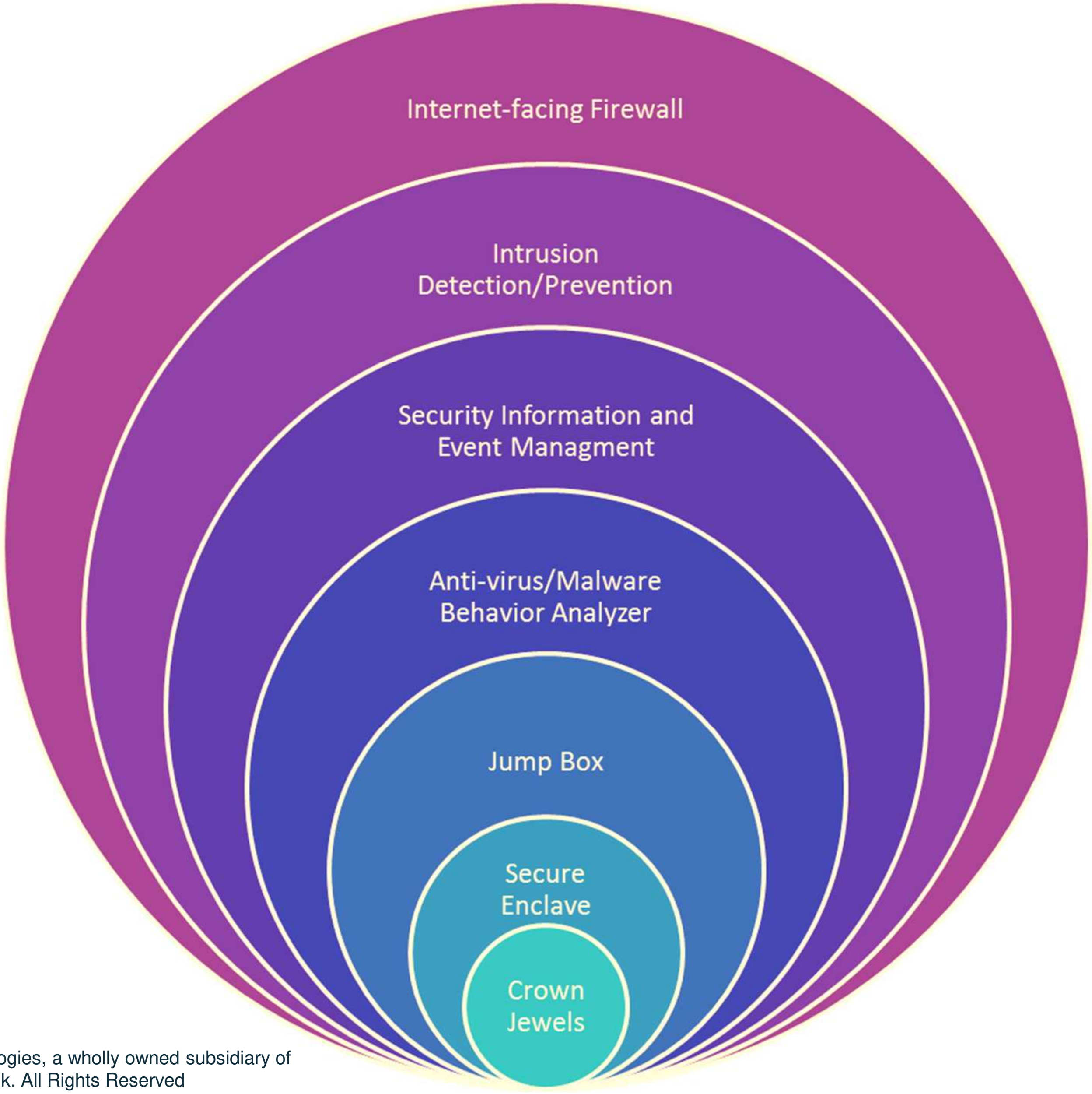
Cybersecurity Plans:

WHAT CAN *YOU* DO?

The Basics

- Who has access?
- What is on the network?
- Where is the data?
- What has the most value?

Defense!


Internet-facing Firewall
Intrusion Detection/Prevention
Security Information and Event Managment
Anti-virus/Malware Behavior Analyzer
Jump Box
Secure Enclave
Crown Jewels

Cybersecurity Tips – Share With Your Teams and Students!

- Realize that you and your teams are an attractive target to hackers. Don’t ever say *“It won’t happen to me.”*
- Practice good password management. Use a strong mix of characters, and don’t use the same password for multiple sites. Don’t share your password with others, don’t write it down, and definitely don’t write it on a post-it note attached to your monitor.
- Never leave your devices unattended. If you need to leave your computer, phone, or tablet for any length of time—no matter how short—lock it up so no one can use it while you’re gone.
- If you keep sensitive information on a flash drive or external hard drive, make sure to lock it up as well and encrypt it.
- Never click on a link in an email. If it’s unexpected or suspicious for any reason, just delete the email. Double check the URL of the website the link takes you to: bad actors will often take advantage of spelling mistakes to direct you to a harmful domain.

Cybersecurity Tips – Share With Your Teams and Students!

- Back up your data regularly, and make sure your anti-virus software and operating system is always up to date. Set those programs to update automatically.

- Be conscious of what you plug in to your computer. Malware can be spread through infected flash drives, external hard drives, and even smartphones.

- Watch what you’re sharing on social networks. Criminals can befriend you and easily gain access to a shocking amount of information—where you go to school, where you work, when you’re on vacation—that could help them gain access to more valuable data.

Cybersecurity Tips – Share With Your Teams and Students!

- Offline, be wary of social engineering, where someone attempts to gain information from you through manipulation. If someone calls or emails you asking for sensitive information, it’s okay to say no.

- Be sure to monitor your accounts for any suspicious activity. If you see something unfamiliar, it could be a sign that you’ve been compromised.

- Be suspicious, slow down. Criminals count on your being too busy or distracted to really look at that email or website.

Recap

- Prevention
  - Solutions, policies and procedures need to be identified to reduce the risk of attacks

- Resolutions
  - In the event of a computer security breach, plans and procedures need to be in place to determine the resources that will be used to remedy a threat

- Restitutions
  - Institutions need to be prepared to address the repercussions of a security threat with their employees and students to ensure that any loss of trust is minimal and short-lived

THANK YOU!

Diane McCracken, EVP, Chief Security Officer - BankMobile
Ray Parris, Vice President of Sales - BankMobile

BankMobile