500 MILLION BLOCKED THREAT MESSAGES: IT SECURITY UPDATE

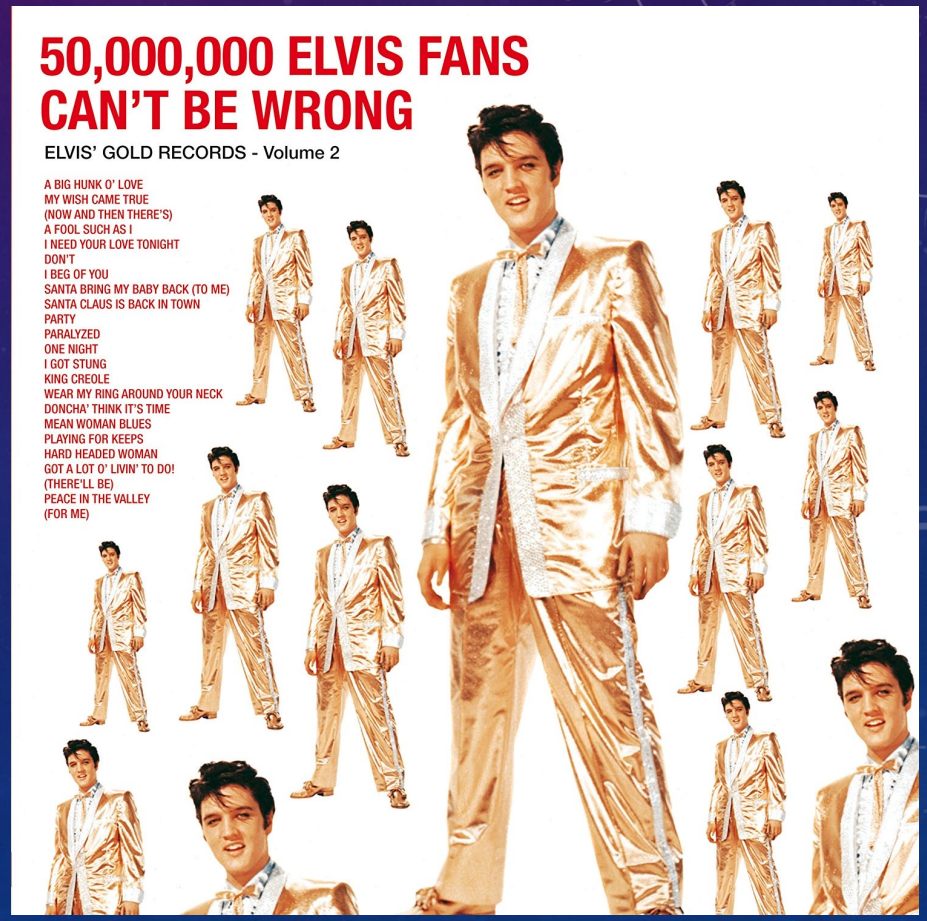
ERNIE SOFFRONOFF

DIRECTOR, WSE IT

ERNIE.S@JHU.EDU

A BIG SCARY NUMBER!

- In 2020, 61% of email blocked at Internet border before going to mailboxes
- That's actually down from 2017, when about 75% of email was blocked
- There are about a dozen layers of protection to traverse for email messages coming from outside JH
- Other tools to clean up threat messages that do make it through
- Ten times more blocked email than Elvis fans?



REMEMBER:

Everything discussed here as being good for Hopkins also applies to your own personal online security.

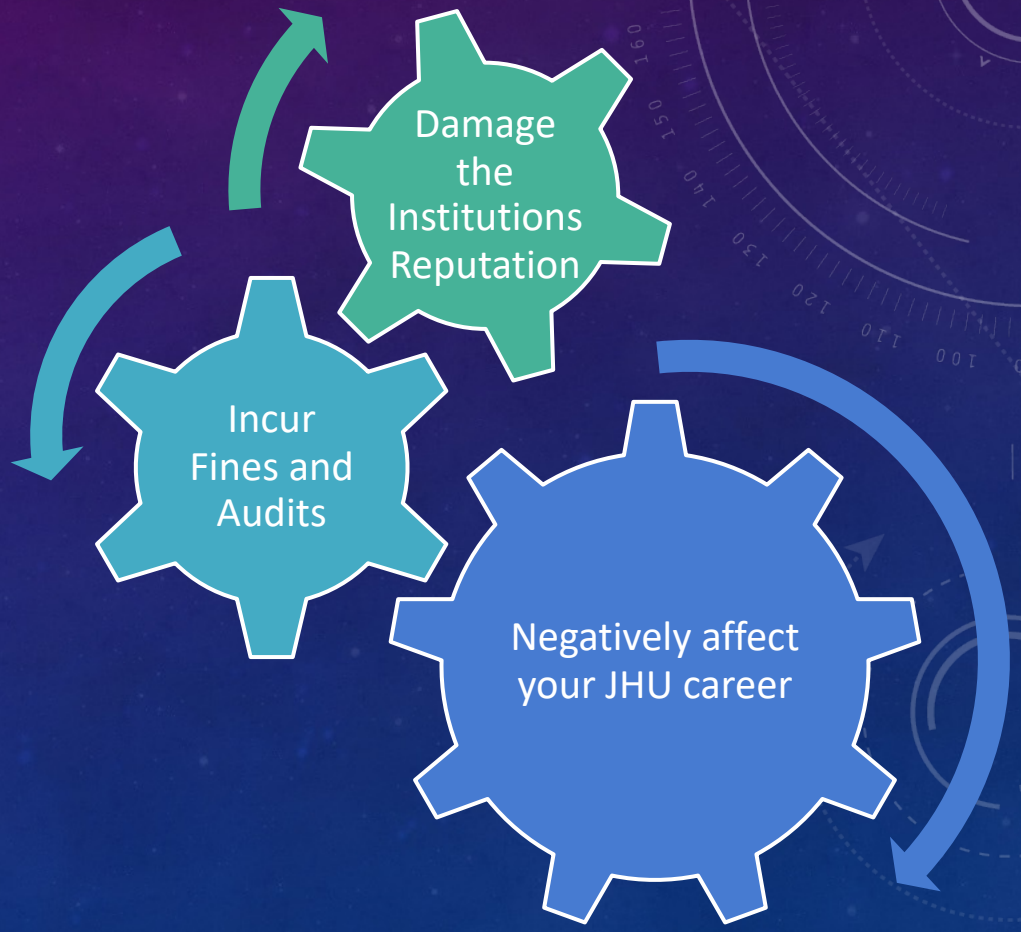
AGENDA

- Terminology
- Are the threats real?
- What are our risks?
- What should we do?
- Questions?

TERMINOLOGY

WHAT IS IT SECURITY?

- We are considering Confidentiality, Integrity, and Availability
- Not everything needs to be secure, but it's important we **understand and accept the risks** of the degree of security applied
- How would you want this handled if it was YOUR information?



WHAT IS PERSONALLY IDENTIFIABLE INFORMATION?

It includes, but is not limited to:

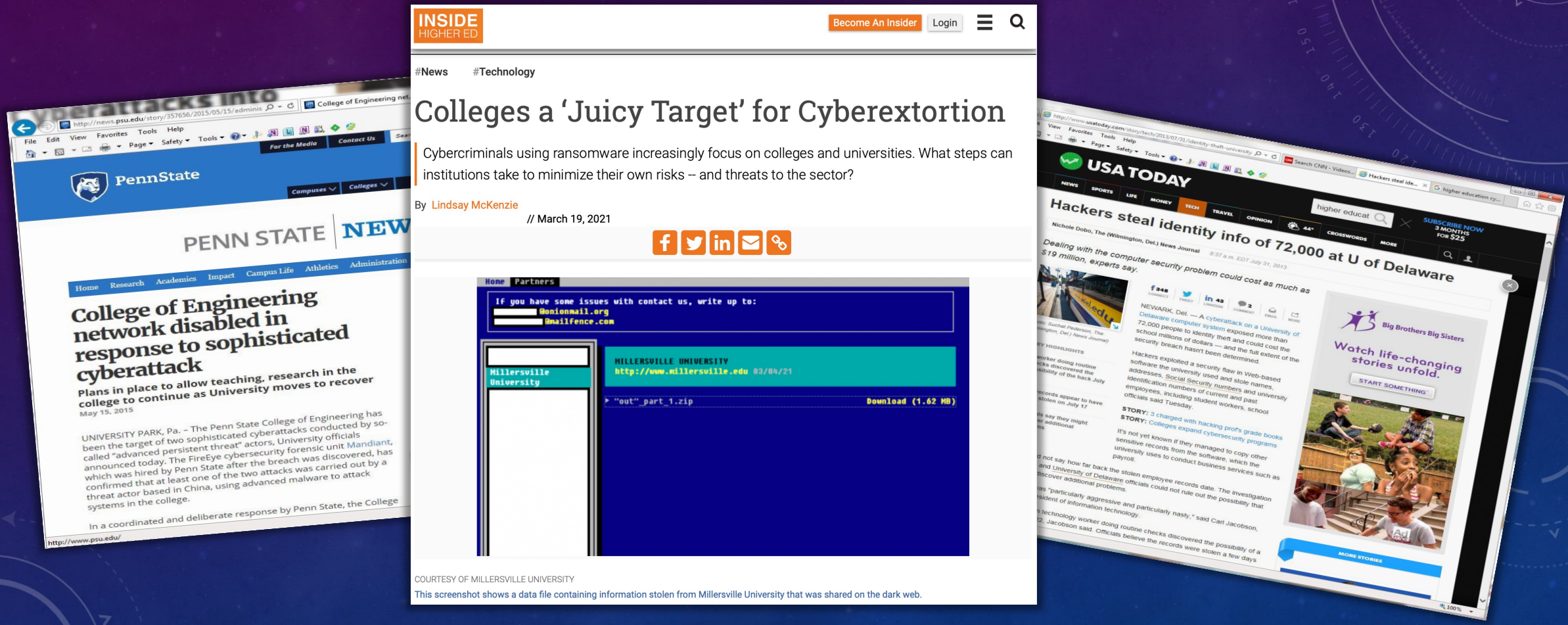
- SSNs
- Dates of Birth
- Financial Account Information
- Driver's License Numbers
- Credit Card Numbers
- Health Information

PII is often more sensitive in combinations than in isolation:

- Email address: not sensitive
- Last four of SSN: not (that) sensitive
- Together? Very sensitive!

ARE THE THREATS REAL?

HIGHER EDUCATION CYBER ATTACKS



PennState

PENN STATE | NEW

Home Research Academics Impact Campus Life Athletics Administration

College of Engineering network disabled in response to sophisticated cyberattack

Plans in place to allow teaching, research in the college to continue as University moves to recover

May 15, 2015

UNIVERSITY PARK, Pa. – The Penn State College of Engineering has been the target of two sophisticated cyberattacks conducted by so-called "advanced persistent threat" actors, University officials announced today. The FireEye cybersecurity forensic unit Mandiant, which was hired by Penn State after the breach was discovered, has confirmed that at least one of the two attacks was carried out by a threat actor based in China, using advanced malware to attack systems in the college.

In a coordinated and deliberate response by Penn State, the College

INSIDE HIGHER ED

Become An Insider Login

#News #Technology

Colleges a 'Juicy Target' for Cyberextortion

Cybercriminals using ransomware increasingly focus on colleges and universities. What steps can institutions take to minimize their own risks -- and threats to the sector?

By Lindsay McKenzie

// March 19, 2021

Home Partners

If you have some issues with contact us, write up to:

[redacted]@onionmail.org

[redacted]@mailfence.com

Millersville University

MILLERSVILLE UNIVERSITY

http://www.millersville.edu 03/04/21

"out"_part_1.zip Download (1.62 MB)

COURTESY OF MILLERSVILLE UNIVERSITY

This screenshot shows a data file containing information stolen from Millersville University that was shared on the dark web.

USA TODAY

Hackers steal identity info of 72,000 at U of Delaware

Dealing with the computer security problem could cost as much as $19 million, experts say.

NEWARK, Del. — A cyberattack on a University of Delaware computer system exposed more than 72,000 people to identity theft and could cost the school millions of dollars — and the full extent of the security breach hasn't been determined.

Hackers exploited a security flaw in Web-based software the university used and stole names, addresses, Social Security numbers and university identification numbers of current and past employees, including student workers, school officials said Tuesday.

STORY: 3 charged with hacking prof's grade books

STORY: Colleges expand cybersecurity programs

It's not yet known if they managed to copy other sensitive records from the software, which the university uses to conduct business services such as payroll.

Big Brothers Big Sisters

Watch life-changing stories unfold.

START SOMETHING

ABOUT BREACHES

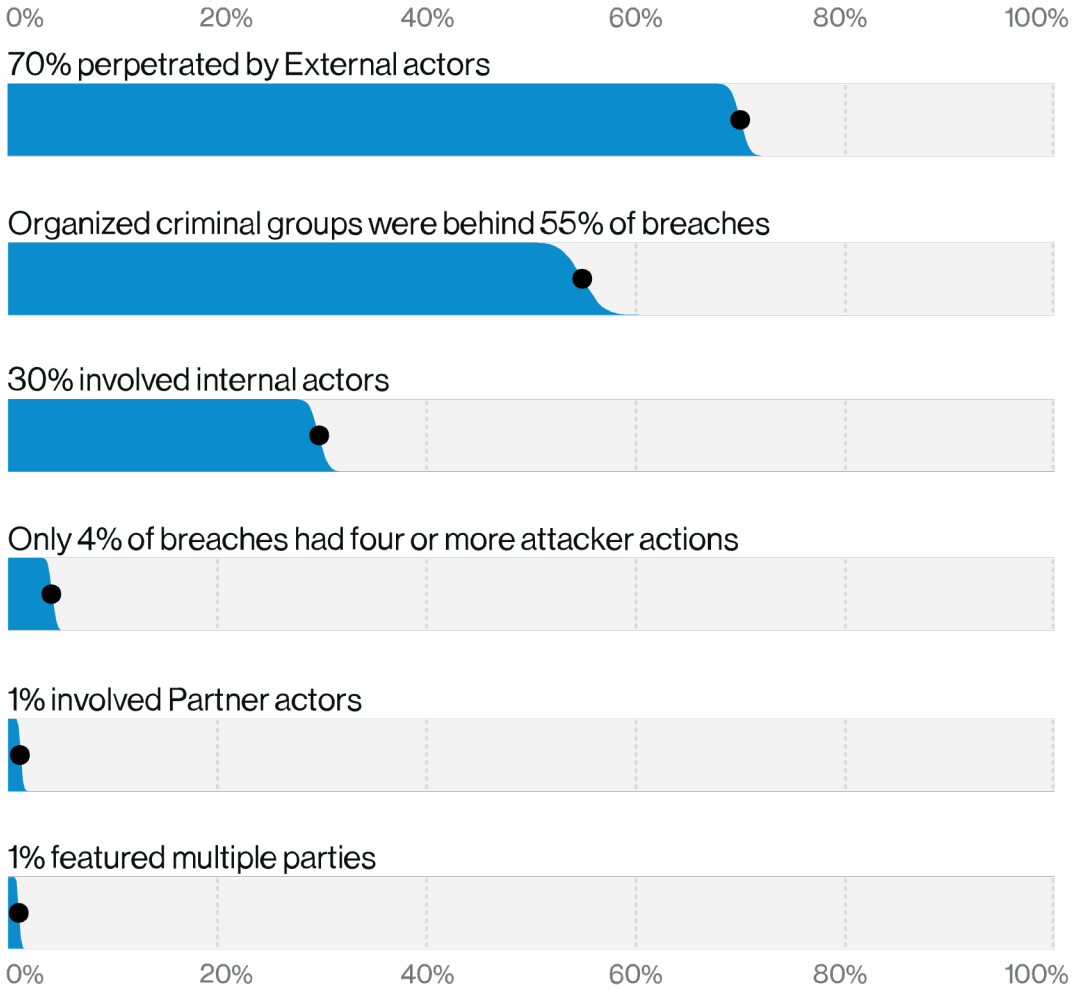


Figure 3. Who's behind the breaches?

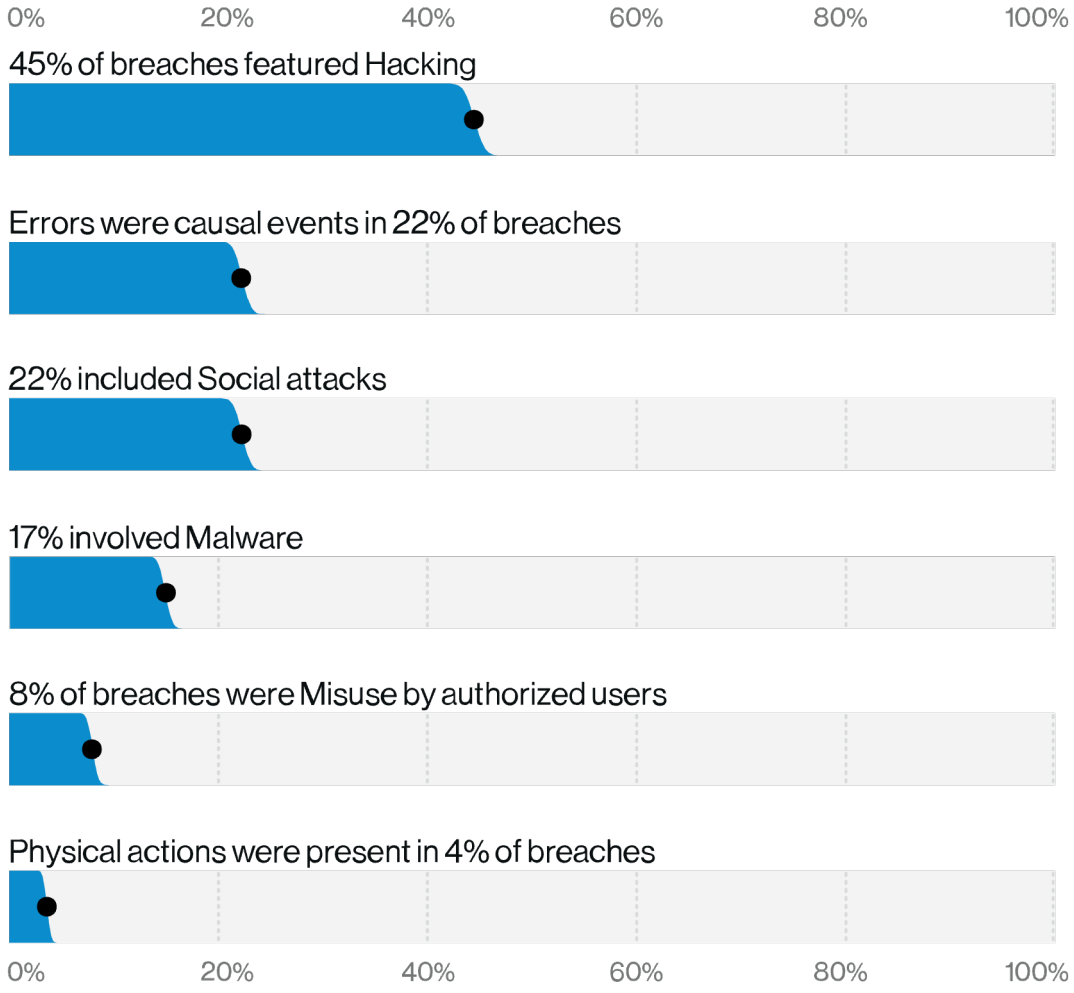


Figure 2. What tactics are utilized? (Actions)

Source: Verizon 2020 Data Breach Investigation Report

MORE ABOUT BREACHES

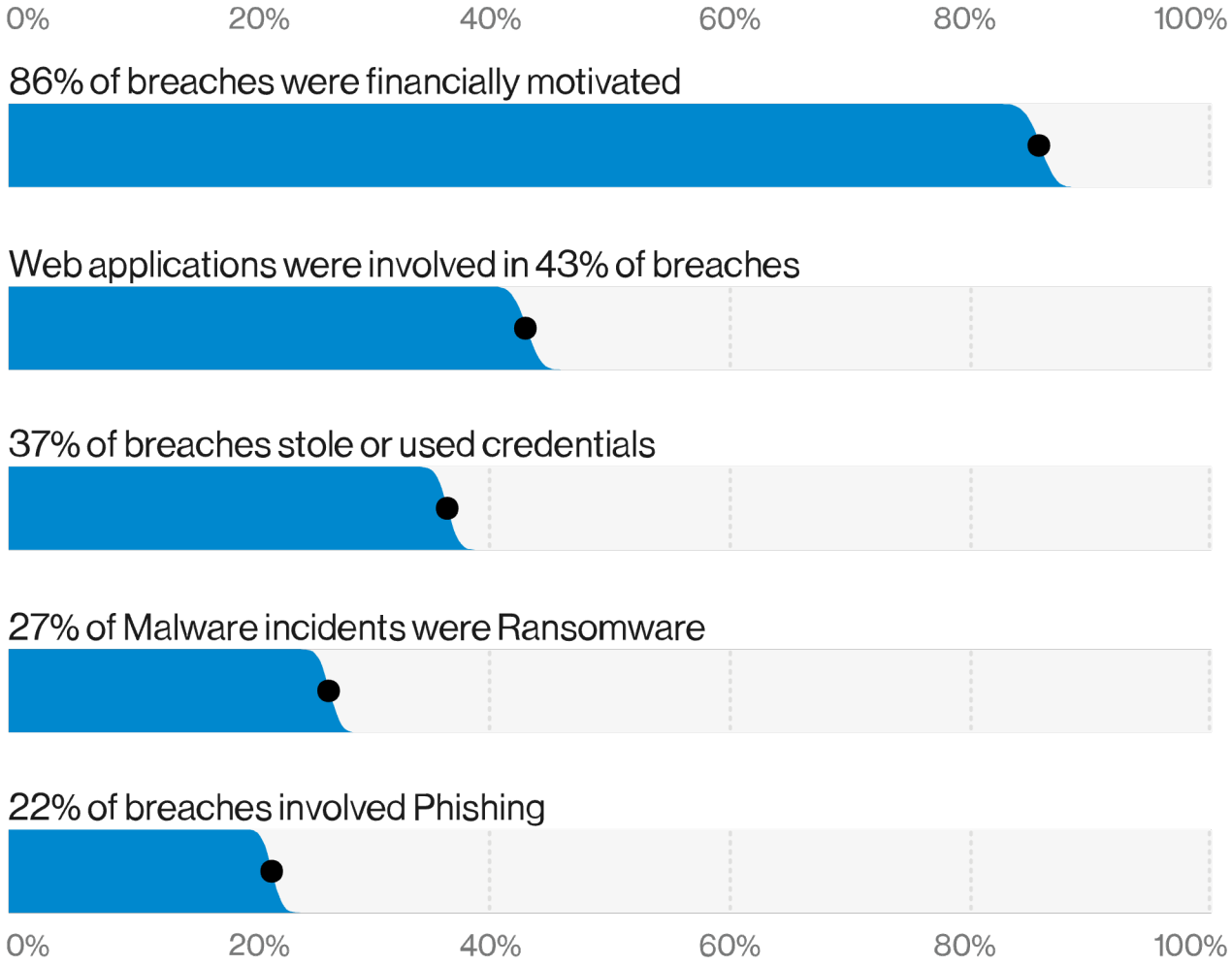


Figure 5. What are the other commonalities?

Frequency

819 incidents, 228 with confirmed data disclosure

Top Patterns

Miscellaneous Errors and Web Applications represent 81% of breaches

Threat Actors

External (67%), Internal (33%), Partner (1%), Multiple (1%)

Actor Motives

Financial (92%), Fun (5%), Convenience (3%), Espionage (3%), Secondary (2%)

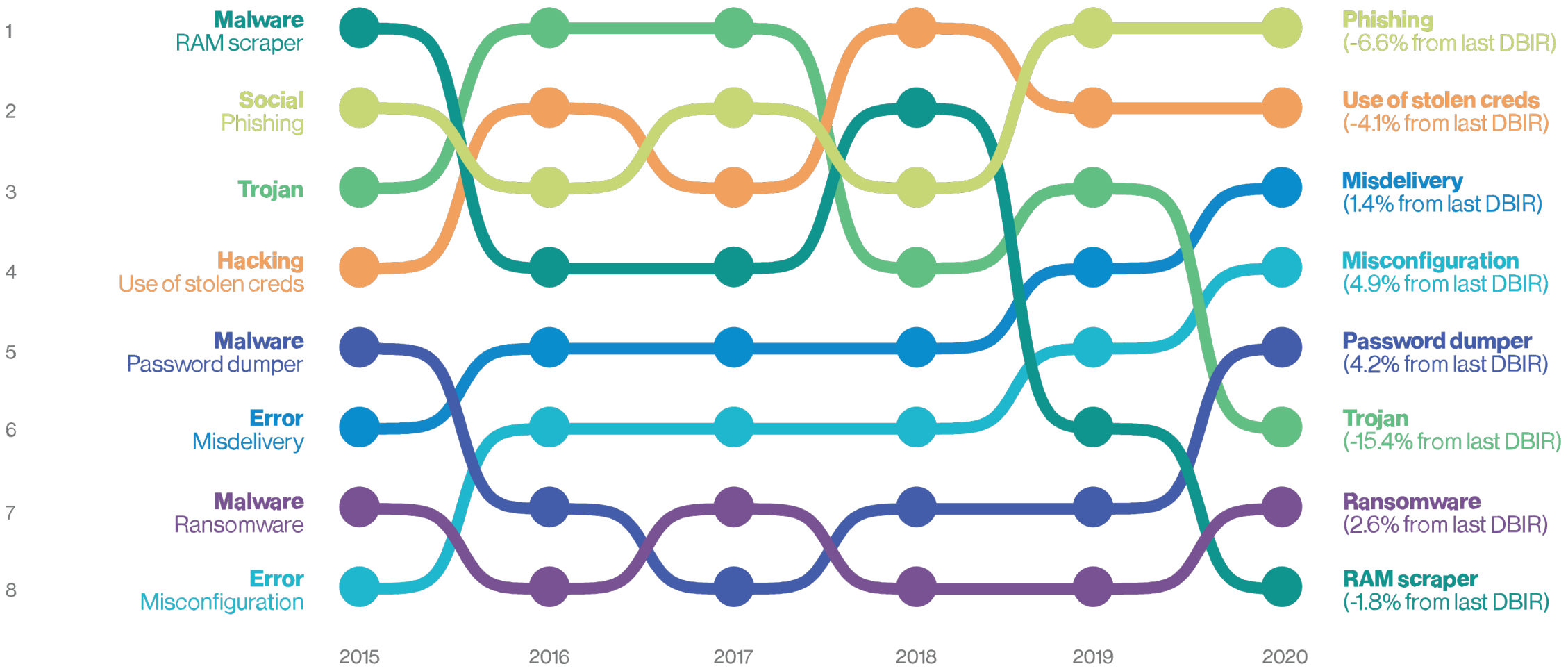
Data Compromised

Personal (75%), Credentials (30%), Other (23%), Internal (13%)

Source: Verizon 2020 Data Breach Investigation Report

MORE ABOUT BREACHES

Figure 6. Select action varieties in breaches over time



Source: Verizon 2020 Data Breach Investigation Report

WHAT ARE OUR RISKS?

PHISHING… TAX FRAUD…

IT at Johns Hopkins
Phishing scams continue to be aimed at Johns Hopkins
To: Ernie Soffronoff,
Reply-To: IT at Johns Hopkins

Is this email not displaying correc

JOHNS HOPKINS
UNIVERSITY & HEALTH SYSTEM

Dear Colleagues:

Members of the Johns Hopkins community are being targeted by a phis
email appearing to be from Johns Hopkins IT asks you to click a link to
This link takes you to a fake page intended to trick you into providing yo

This is the latest in a series of phishing scams intended to deceive peo
are responding to an official Johns Hopkins request. To protect your pe
the security of Johns Hopkins' systems, please be extremely cautious a
asks you to follow a link and enter your login or other personal informat

Know what to look for

The new phishing email looks like this screenshot:

From: JHED IT [mailto:jhedsupport@comcast.net]
Sent: Wednesday, January 18, 2017 1:23 PM
Subject: Secure Validation

Michelle Thompson Inbox - Hopkins July 14, 2017 at 10:31 AM
Equifax/TALX W2 Details
To:

Dear Liaisons:

As we discussed in a recent meeting, Hopkins is sending out letters to individuals that have either self-reported 2017 tax fraud or for whom we have ide
this in your organization. Any f
below. In a few weeks, Wanda

Late Wednesday, a firm workin
spring (under the signatures o
University personnel but also t

For questions or concerns, ple

1) You should first direct them
IDExperts is able to efficiently
939-4170.

2) If the caller insists on talkin
the address below (even if the
individuals to contact IDExpert

tax.office@jhu.edu

3) If you or another administra
address. Please try to avoid se
office and will be for the next s

4) Some people may try to cal
investigations conducted on th
IDExperts may not be able to
Thanks.

JOHNS HOPKINS
WHITING SCHOOL
of ENGINEERING

January 27, 2021

Dear Johns Hopkins Faculty and Staff,

It's the time of year when preparing to file 2020 income taxes becomes top of mind, and we hav
important updates and information to share with you.

Be aware of scams

We'd like to remind you to please be aware of scams involving W-2s, tax filing, and your persona
information. To avoid being the victim of a scam, please be aware of the following:

- Consider filing your taxes as early as possible, because the IRS allows only one tax retur

CRYPTOLOCKER? WANNACRY?

DISCLOSURE NOTIFICATION

bout JHU | Admissions & Aid | Schools & Divisions | Research & Faculty | Campus Life

Google Custom Se

JOHNS HOPKINS UNIVERSITY

inistration > Office of Communications

ice of Communications
lews Releases
lews by Topic
lews by School
Events
Blue Jays Sports
Contacting News Staff

Return to News Releases

Johns Hopkins Statement: Breac

March 7, 2014
FOR IMMEDIATE RELEASE
CONTACT: Dennis O'Shea
443-997-9912 (office)
410-499-7460 (cell)
dro@jhu.edu

The following statement may be attributed to Johns Hopkins University spoke

Johns Hopkins has learned from the FBI that information stolen from a Depa
posted on the Internet on Thursday, March 6. This came one day after the de
extortion message from someone claiming to be a member of the hackers' gr

The extortionist threatened to post stolen BME Department data if the univers
access the university's network. The university did not and will not provide th

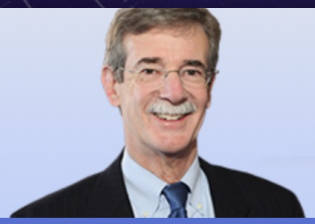
The department, the Whiting School of Engineering and the university are inv
FBI's criminal investigation. We are still gathering information, but here is wh

— The server in question is used primarily to produce the Biomedical Engine
occurred late last year, but came to light when someone posted on Twitter in
error that left a database on the server vulnerable was promptly identified an

— There is no evidence that the database on the server contained Social Se

MARYLAND OFFICE OF THE ATTORNEY GENERAL

BRIAN E. FROSH
MARYLAND ATTORNEY GENERAL



FILE A CONSUMER COMPLAINT | HOME | SERVICES | REGISTRATIONS | NEWS | OUR OFFICE | EMPLOY

Quick Links

- About Information Security Breaches
- Comprehensive Guide to Identity Theft (PDF)
- Guide to Freezing Your Credit Report
- Identity Theft Passport
- Protect Yourself From Identity Theft
- Unemployment Insurance Fraud

Maryland Information Security Breach Notices

- Security Breach Notices

Businesses

- Digital Copier Security
- Guidelines for security breach

Maryland Information Security Breach Notices

As of January 2008, any business that retains consumer records is required by Maryland law to notify a consu
resident of Maryland if his or her information is compromised. The "security breach law" also requires the busi
the Office of the Attorney General. Links to notices sent to the OAG from 2017 to the present are listed on this
are working to keep this list as up-to-date as possible. Questions about specific notices may be directed to
IDTheft@oag.state.md.us. Below is a chart containing the case number, date of the notice, business name, h
people are affected what information was compromised and how it was lost.

Find a file

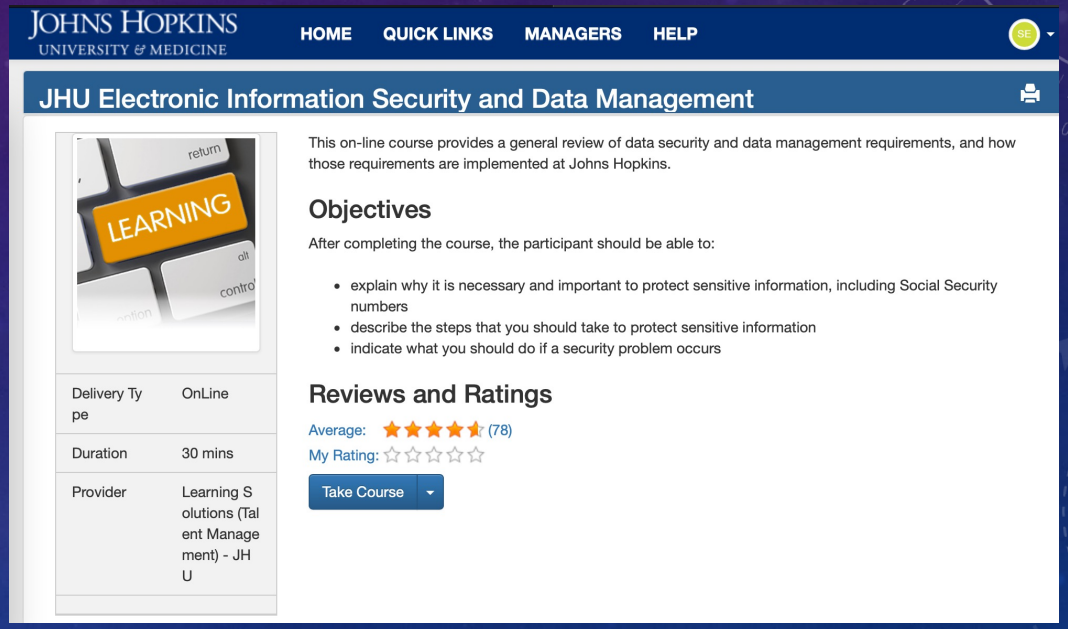
Case Title	Case No.	Date Received	No of MD Residents	Information Breached	How
Year : 2020 (951)					
World Vision, Inc.	itu-331763	8/31/2020	4	name, contact information, email, physical mailing address, ssn driver' license number, financial account information, and date of birth	rans atta occu Feb thro 202

WHAT SHOULD WE DO?

VERIZON 2020 DATA BREACH INVESTIGATION REPORT TOP CONTROLS FOR EDUCATION

1. Implement a Security Awareness and Training Program
2. Boundary Defense
3. Secure Configuration – PLEASE REBOOT WEEKLY

NEW: MyLearning "JHU Electronic Information Security and Data Management"



Problem	Responses
Phishing (or other threat) Email	• Healthy skepticism • Look for traits of “real” login page • Forward messages to spam@jhu.edu • Don’t use external mailbox (Gmail) for work email
Stolen Credentials	• Multi-factor authentication • Don’t reuse passwords • Password rotation, password quality • Notifications on account activity
Malware and Cryptolocker	• Keep patches up to date • Back up files to server, or use desktop backup • Use OneDrive • Be mindful of what networks you connect to
Information Disclosure	• Minimize retained data in scope and time • Encryption for devices • Share data using OneDrve, [secure] email service • Hygiene for your desk (shred papers, lock workstation)

CAN YOU LIMIT WHAT DATA COULD BE LEAKED?

From this:

Name	JHED	Birthdate	SSN
Person, Newest	nperson7	August 19, 1999	012-34-5678
Person, Middle	mperson4	March 25, 1985	876-54-3210
Person, Oldest	operson1	June 5, 1970	123-45-6789

To this:

Name	JHED	Birthdate	SSN
Person, Newest	nperson7	(redacted)	5678
Person, Middle	mperson4	(redacted)	3210
(redacted)	(redacted)	(redacted)	(redacted)