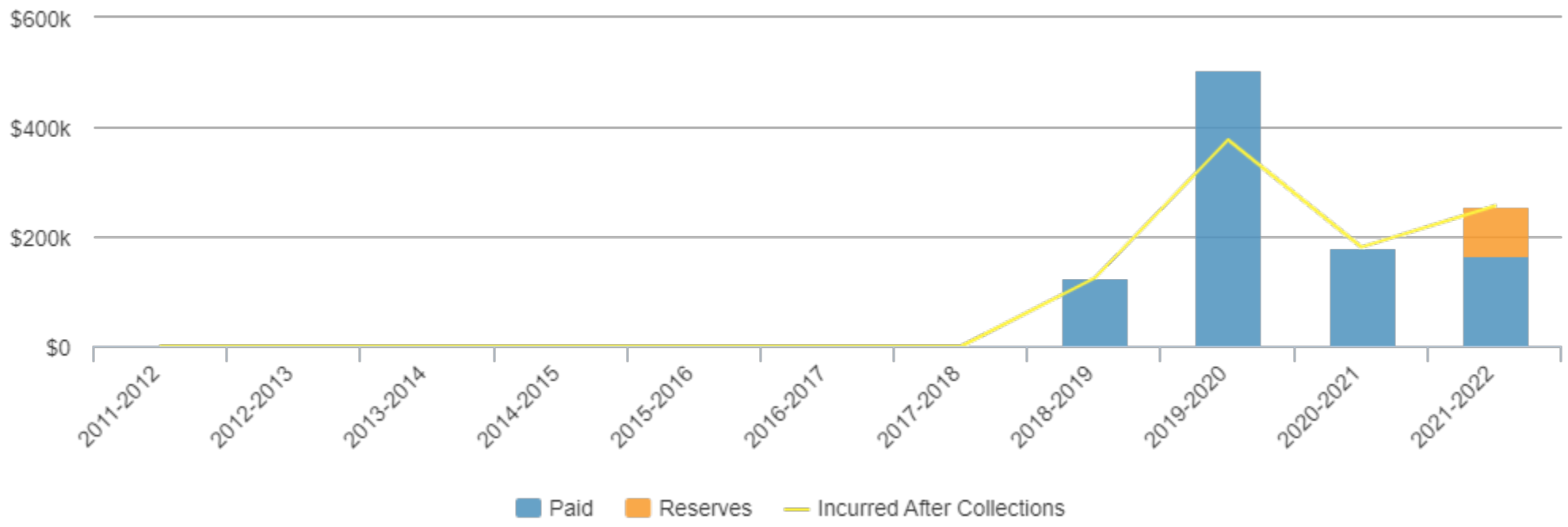
CIS Cyber Claims



INFORMATION TECHNOLOGY

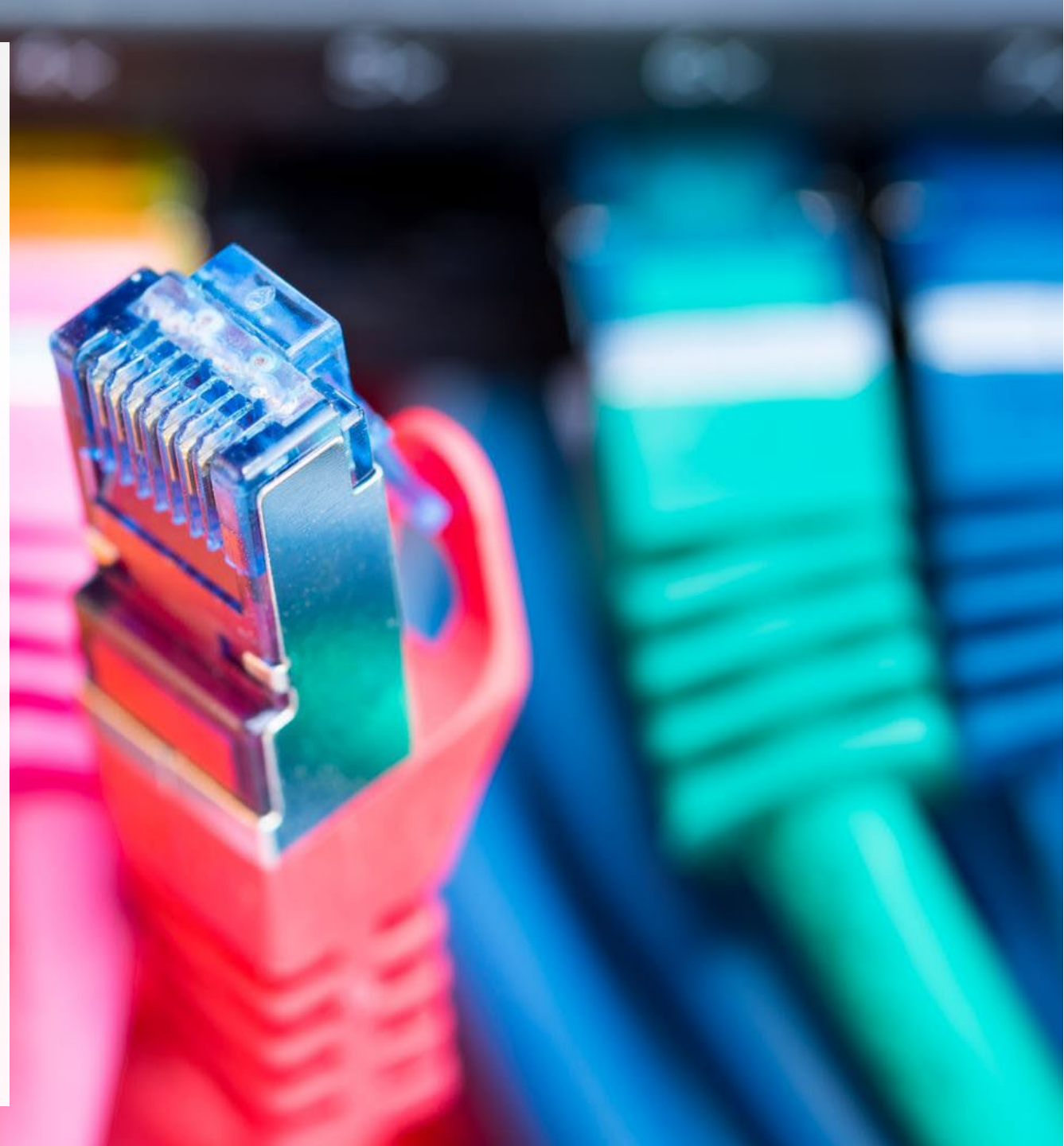
2019 INCIDENT

How it Began

- Phishing Email from the “Police Chief” asking our Communications Officer to “check out this story”
- Email address appeared normal in Outlook, but the actual address it came from was incorrect
- Employee clicked on the “link” and instantly downloaded the client

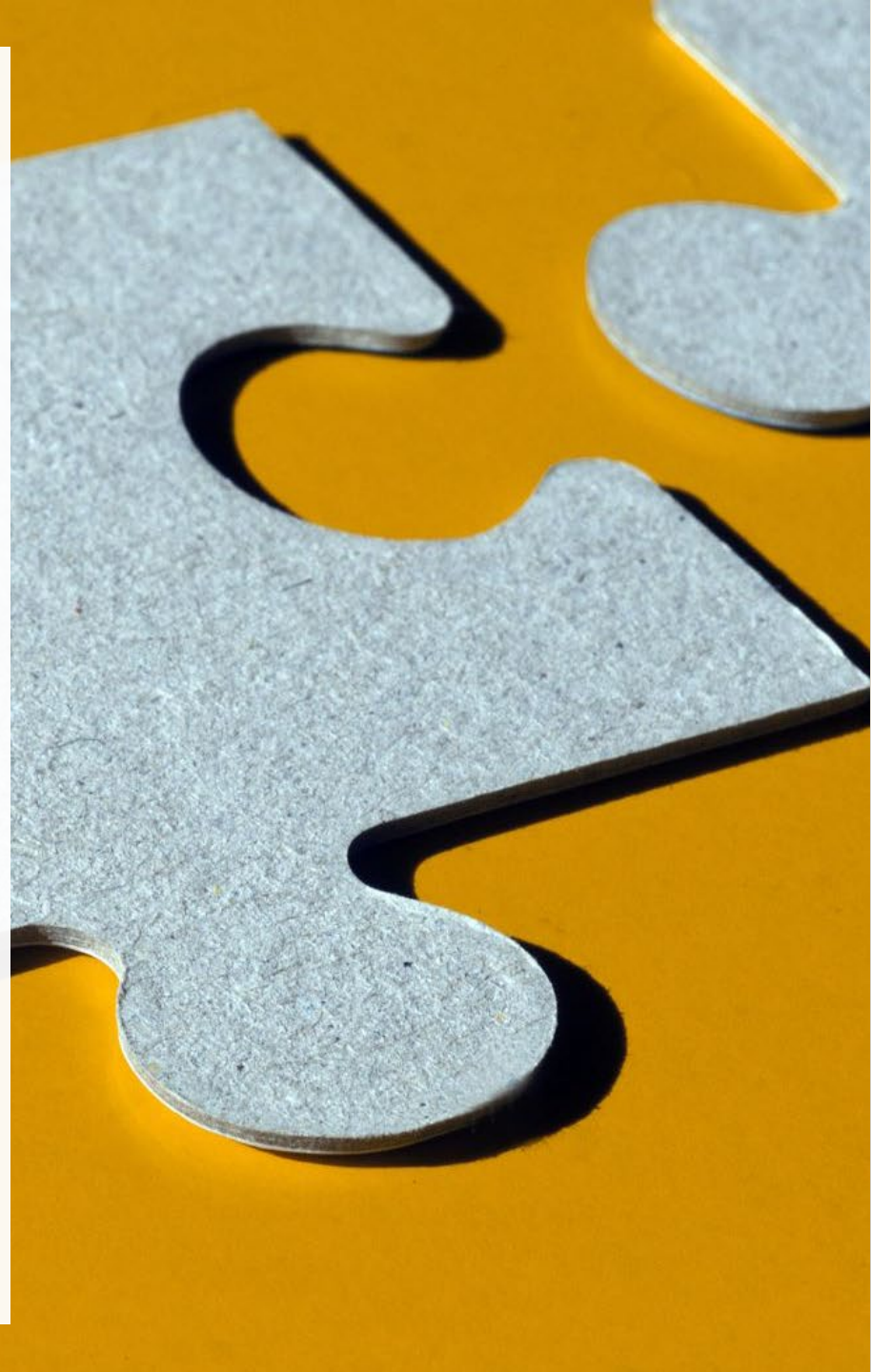
Chaos Ensued

- IT management company noticed unusual activity during a routine IT overview and caught hackers “in the act” of copying data
- Literally RAN to the server room to unplug everything
- Ransomware was found on the main server
- CIS Insurance took over



IT Audit

- CIS Insurance brough a 3rd party IT investigation team to help assess the situation.
- Audit found several weakness points of concern:
  - Password Configurations among users and admins
  - Email filters/safeguards turned “off” by IT Management on several computers (including the “host” computer)
  - Ineffective virus software (old & outdated)
  - Server access not effectively protected or “scrubbed” in several years. Contained MANY old and inactive users
  - Over 85% of computers in the city were affected in some capacity by the ransomware



End Game

- Changed IT service provider & currently working towards in-house IT management for more control
- Replaced ALL computers and laptops at the City over 3-6 months starting with essential employees
- Instituted tighter Admin controls, backup policies, and an advanced virus protection software (Sentinel One)
- Working towards ongoing IT Audits and penetration testing among staff
- VERY LUCK to catch things early by mistake


Cyber Case Study
InterMountain
EDUCATION SERVICE DISTRICT


the one with GOOD NEWS
City of
La Grande
OREGON

Setting the Scene

June 2020 – Many staff working from home due to pandemic

A City employee who works with sensitive information has a new personal HP printer at home

Employee contacts HP for assistance setting up the printer on City provided computer

The person on the other end of the call was unable to assist with the setup and the call was ended

Ring Ring...

The employee later receives a call from “HP” asking to remotely access to the computer to provide support

The employee agrees and grants the person access

Fake HP support spent time controlling the computer appearing to “help” with the printer

The employee was informed the computer didn’t have anti-virus software (it did)

Fake HP support attempted to obtain payment information from the employee to sell some “excellent” anti-virus software

The employee immediately ended the call and remote-control session and alerted City IT Staff

the good, the bad, and the LUCKY

We knew an unauthorized external actor conned their way onto a City computer

What did they do while they had access?

IT quarantined the computer and placed retention holds on server backups to maintain evidence

The employee's password was changed

The City contacted CIS who engaged an IT forensic investigation group

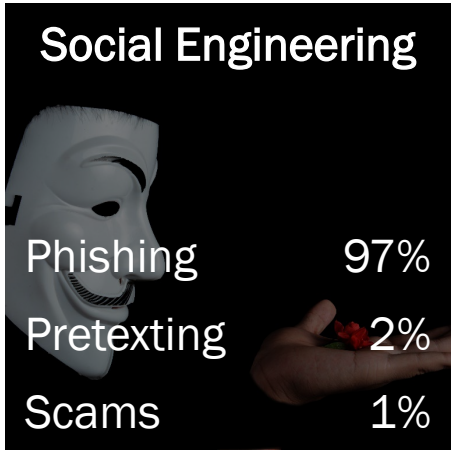
The forensic group was unable to find evidence that would trigger any breach notification laws

Fake HP support was after money for their "anti-virus" software

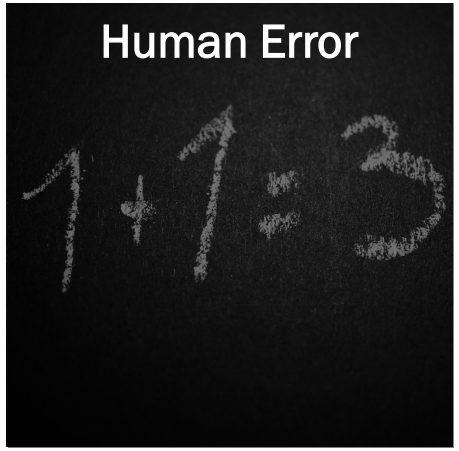
2021 Breach Vectors

in

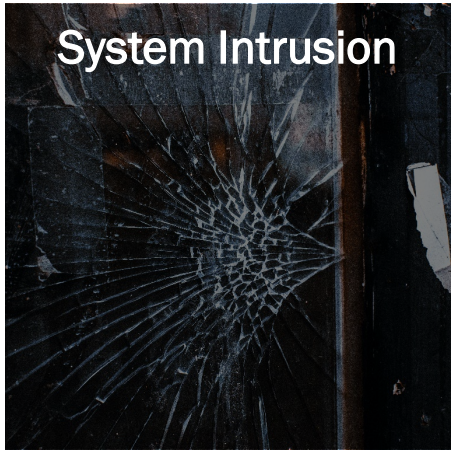
Public Administration & Government Sector



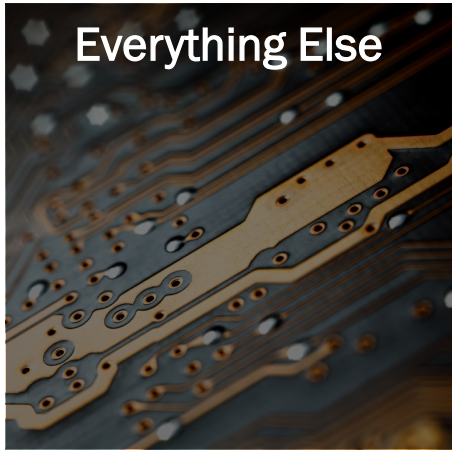
69%



14%



9%



8%

*Source: 2021 Verizon Breach Investigations Report

CYBERSECURITY

a journey without a final destination

Raise awareness & train staff

Use tools like KnowBe4

Practice makes perfect

Develop & adopt information security / cybersecurity policy

Develop & practice incident response plan

Remove administrative rights on computers

Implement Endpoint Detection and Response (EDR)

Conduct IT security audits

Implement Multi-Factor Authentication (MFA)

Conduct daily backups and monthly test restores (3-2-1 rule)

Regularly update (patch) IT systems

Update/replace legacy systems

Join MS-ISAC!

Know where you are

Know where you need to go

Prioritize and take building block approach

there's no time like the **PRESENT**

Nick Lapp, CISSP, CGEIT, CDPSE
Chief Technology Officer
InterMountain ESD
Nick.Lapp@imesd.k12.or.us
541.966.3183

InterMountain
EDUCATION SERVICE DISTRICT

CIS Cyber Coverage

- $50,000 primary layer (Tier 1)
- $250,000 layer (Tier 2)
- Excess Cyber (Tier 3)
  - $500,000
  - $1,000,000
- New application
- New requirements

CIS Cyber Security Requirements

1. Multi-factor authentication
2. End-point protection, detection, and response (EDR) product implemented across enterprise with 24/7/365 response
3. Backups
4. Adopt CIS Cyber Security Policy or similar
5. Training
6. Testing
6. Critical and high severity patches installed within 30 or fewer days
7. Plan or adequate measures in place to protect end of life software
8. Have at least $250,000 of excess crime insurance for fraudulent instruction coverage

Patrick Priest
CIS Executive Director
800-922-2684, ext. 3810
ppriest@cisoregon.org