

# Ransomware

**Jim Basney**

Director, Trusted CI

[jbasney@ncsa.illinois.edu](mailto:jbasney@ncsa.illinois.edu)

MS-CC Cybersecurity Community of  
Practice

October 10, 2023

# Growing Ransomware Risk to Science

Ransomware has changed the cybercrime landscape, broadly expanding potential victims to include hospitals, schools, cities, and researchers.

Trusted CI is warning researchers to take the risk seriously and be prepared for business continuity and extortion attacks.

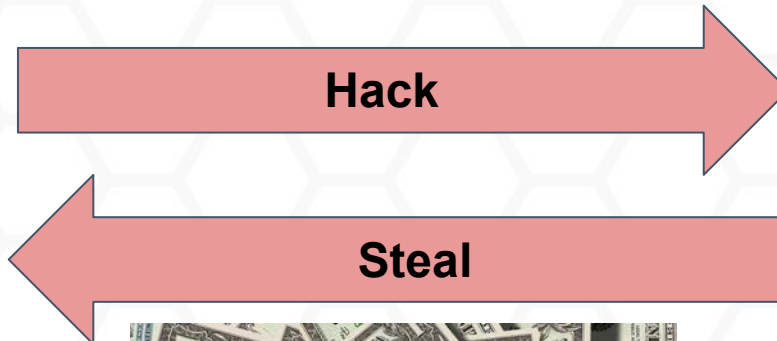
We are collecting resources at:

<https://www.trustedci.org/ransomware>



A screenshot of the Trusted CI website page titled "Ransomware". The page header includes the Trusted CI logo, navigation links (About, Community, Services, Resources, Events, Blog, Contact), and a search bar. The main content area is titled "Ransomware" and contains the following text: "Historically, research organizations have been largely ignored by cybercriminals since they do not typically have data that is easily sold or otherwise monetized. Unfortunately, since ransomware works by extorting payments from victims to get their own data back, research organizations are no longer immune to being targeted by criminals. Trusted CI is committed to motivating research organizations to prevent future negative impacts to their research mission." Below this is a section titled "Ransomware lessons learned:" with a bulleted list of resources: "Research at Risk: Ransomware attack on Physics and Astronomy Case Study" (with sub-link for webinar) and "The Technical Landscape of Ransomware: Threat Models and Defense Models" (with sub-link for webinar). The next section is "Technical landscape" with a bulleted list of resources: "REN-ISAC Ransomware Best Practices", "CISA Ransomware Guidance and Resources", and "NIST Ransomware Protection and Response". The final section is "Best practices:" with the same three bulleted resources.

# Traditional Cybercrime: Hack where the money is...



Bank, store, etc.



Cash, CC#s, SSNs, etc.



# Ransomware: Hack the data, then extort the money...

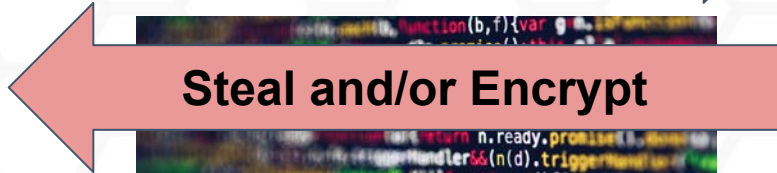


Photo by Nikita Belokhonov: <https://www.pexels.com/photo/anonymous-hacker-with-on-laptop-in-white-room-5829726/>

Photo by Christina Morillo: <https://www.pexels.com/photo/software-engineer-looking-at-an-ipad-1181335/>

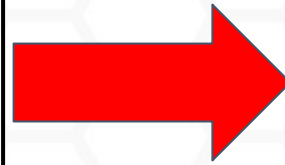
Photo by Pixabay: <https://www.pexels.com/photo/high-angle-view-of-a-man-256381/>

Photo by Markus Spiske: <https://www.pexels.com/photo/codes-on-tilt-shift-lens-2004161/>

## **Traditional Cybercrime**

Banks  
SSNs  
CC#s  
Medical fraud

Those with fungible data  
and, in general, enough  
money to afford strong  
cybersecurity



## **Ransomware**

K-12  
Cities  
Universities  
etc.

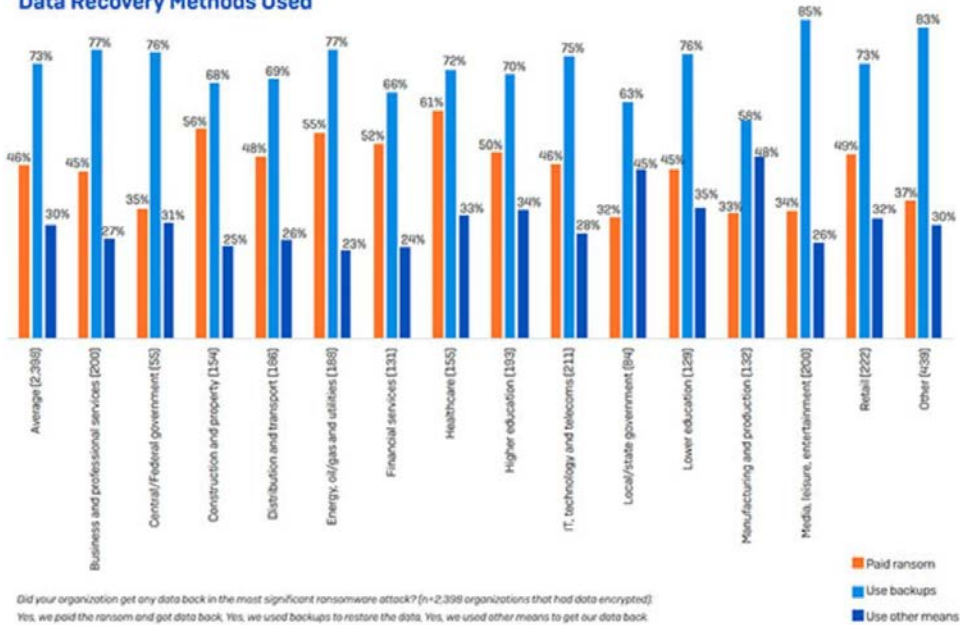
Anyone with data and  
with money, though  
perhaps not enough  
money to afford strong  
cybersecurity

## Ransomware Hit 64% of Higher Ed Institutions Globally in 2021, Sophos Survey Finds

Higher Ed Was Slowest of all Sectors to Recover, State of Ransomware Report Says

- By Kristal Kuykendall
- 04/27/22

### Data Recovery Methods Used



Did your organization get any data back in the most significant ransomware attack? (n=2,398 organizations that had data encrypted)  
 Yes, we paid the ransom and got data back. Yes, we used backups to restore the data. Yes, we used other means to get our data back.

A Sophos Whitepaper, April 2022

## Higher education institutions being targeted for ransomware attacks



by **Brian Stone** in **Security**  
 on May 18, 2022, 2:12 PM PDT

Three colleges have been victims of cyberattacks in the last three months alone.



Image: normalfx/Adobe Stock

While higher education is typically not thought of as a targeted industry for ransomware attacks, a trend may be forming. Three different colleges, North Carolina A&T University, Lincoln College and Austin Peay State University have all been negatively impacted by these types of cyberattacks, with one even leading to the closure of Lincoln College due to the scale of the hack.



# Ransomware Gangs: Who Are They And How To Stop Them



Stu Sjouwerman Forbes Councils Member  
Forbes Technology Council COUNCIL POST | Membership (Fee-Based)

Sep 27, 2021, 09:15am EDT

f *Stu Sjouwerman is the Founder and CEO of KnowBe4 Inc., the world's largest security awareness training and simulated phishing platform.*



GETTY

Cyber-extortion is a thriving trillion-dollar industry run by organized crime syndicates. These ransomware gangs are increasingly becoming more sophisticated, not just in terms of business models but in posturing as corporate entities while simultaneously making extortion demands. These crusaders of crime are trying to gain acceptance as legitimate enterprises, and they're starting to operate as such, coordinating efforts with various partners, offering 24/7 help desks staffed by representatives even branding themselves to hype reputation.

## Sophisticated Attackers

“These crusaders of crime are trying to gain acceptance as legitimate enterprises, and they're starting to operate as such, coordinating efforts with various partners, offering 24/7 help desks staffed by representatives even branding themselves to hype reputation.”

# Most of us are...

A large, relatively open attack surface.

Smaller information security teams than the criminal gangs.

Slower - defense is harder than offense.





Ed Hudson, CISO at California State University, says a 2020 ransomware attack helped his team make improvements to the university's o

HOME >> SECURITY

MAY  
10  
2022

SECURITY

# Universities Share Lessons Learned from Ransomware Attacks



Universities that faced security breaches share advice from their experiences.

by [Chris Hayhurst](#)

Chris Hayhurst is a freelance writer who covers education technology and healthcare, among other topics. He's a regular contributor to the CDW family of technology magazines

▶ LISTEN 07:53

Ed Hudson remembers the incident as if it were yesterday.

It was Oct. 1, 2020, recalls Hudson, the CISO at [California State University](#). The largest four-year public university system in the country, CSU has 23 campuses, nearly half a million students, and close to 50,000 faculty and staff. That day, the IT security team at one of those campuses, [CSU San Marcos](#), discovered that hackers had infiltrated its internal network.

“Build a collaborative network. [California State University] maintains close relationships with state and federal threat intelligence agencies, and with higher ed-focused cybersecurity organizations like EDUCAUSE and REN-ISAC.”

# Let's work together...

We can share intelligence and practices.

REN-ISAC: Research & Education Networks  
Information Sharing & Analysis Center

[https://www.ren-isac.net/public-resources/Ransomware\\_Best\\_Practices.html](https://www.ren-isac.net/public-resources/Ransomware_Best_Practices.html)



# Let's Discuss

For more info:  
<https://www.trustedci.org/ransomware>