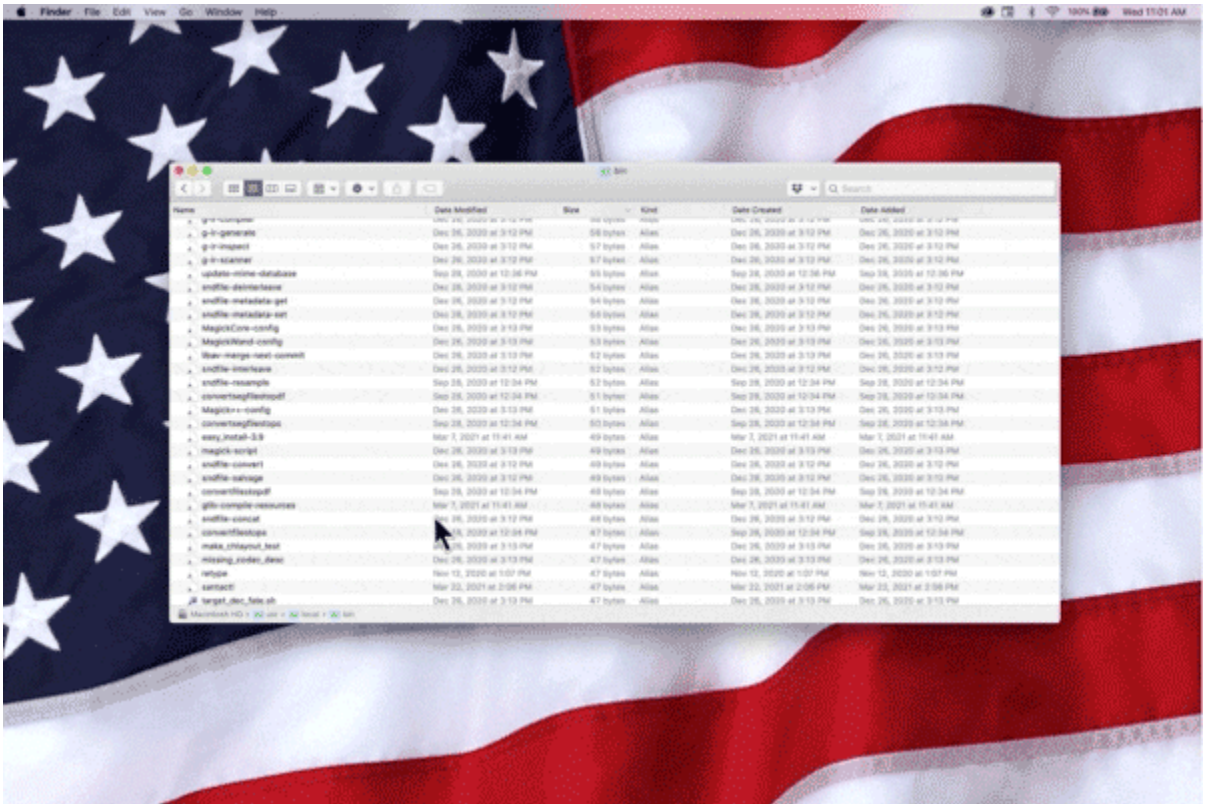
Don’t ignore ransomware. It’s bad.



Adam Ferriss

By Shira Ovide

Ransomware attacks can be devastating, and they’re only getting worse.

This form of cybercrime involves hackers breaking into computer networks and locking up digital information until the victim pays for its release. Hospitals crippled by ransomware attacks have been forced to turn away patients, and a natural gas pipeline was forced offline for two days last year.

My colleague Nicole Perlroth has spent years chronicling the proliferation of cyberattacks, including ransomware. She spoke to me about steps that the U.S. government and individual organizations could take to better prevent it. Nicole tried to be hopeful but she has a discouraging diagnosis of ransomware’s root cause: America has failed to invest in its defense.

Shira: Have ransomware attacks become more common or does it just seem that way?

Nicole: It has gotten worse. We've seen a surge in attacks, more types of organizations targeted and ransom demands up to the tens of millions of dollars. And ransomware gangs are hitting us in ever more visceral ways.

The pandemic made things worse. Companies, schools and other organizations had to accommodate employees working virtually. That created more opportunity for criminals.

Just in the last few months in the United States, ransomware gangs have hit big businesses, schools and universities, local governments, hospitals and the police. And they're getting more brazen. A relatively new twist is criminals threatening to release organizations' data publicly if they don't pay.

What are some of the consequences of ransomware attacks?

Criminals recently targeted a police department in Florida and leaked records including a folder labeled "dead" with photos of bodies from crime scenes.

The worst that I've seen happened at the University of Vermont Medical Center. The hospital couldn't treat some chemotherapy patients because an attack wiped their records. Nurses said it was one of the worst experiences of their careers.

How can anyone justify hurting cancer patients or leaking photos of dead people?

I have no words for this that could be printed in a family newspaper.

What is the United States doing to stop or slow ransomware?

We're not trying very hard. The United States is the most targeted country by cybercriminals and nation states, but we're not acting like it. We're mostly outlining guidelines for companies and government agencies to prevent ransomware attacks and hoping for the best. It's not working.

What should be done instead?

There is no silver bullet, but there are some steps that could help. The U.S. government could designate ransomware as a national security threat on par with terrorism, which would funnel more intelligence resources to combat it. Countries that are safe havens for ransomware gangs such as Russia could be subject to sanctions or restrictions on travel to the

United States. That would pressure countries to go after ransomware criminals inside their borders.

We could also require that companies and government agencies that are hit by ransomware attacks disclose them publicly. The Treasury Department could consider prohibiting victims from paying ransoms. Most ransomware gangs demand payment in Bitcoin, and it could help trace criminals if banking industry "Know Thy Customer" rules and anti-money-laundering laws were enforced with cryptocurrency exchanges.

And we need a 911-type hotline for ransomware victims. Organizations often don't know who to call when they are targeted.

What can organizations that are targeted by ransomware attacks do to prevent them?

If companies, government agencies and organizations required all employees and others who access their computer networks to use strong passwords, password managers and multi-step authentication, it would go a long way to prevent cyberattacks.

It would also help if organizations were required to have copies of their digital records and to back them up regularly. Victims wouldn't be in the position to have to pay to recover their own data. The government could also create tax credits or other financial incentives for companies and government agencies to take those steps.

I don't want to blame victims, but why aren't companies and public agencies taking those protection measures already?

A lot of essential services are operated by small organizations that don't have the resources or the capabilities to even do the basics. American hospitals, schools and governments are common ransomware targets because they tend to use older software with security holes that can't be repaired.

This sounds grim.

I don’t want people to feel hopeless. But yes, ransomware and other cyberattacks are only going to get worse. The central problem is America’s lack of urgency and investment to protect digital systems.