THE WALL STREET JOURNAL.

veeAM

Don't become a ransomware headline.

Keep your business running with the global market leader in data protection and ransomware recovery.

LEARN MORE

Why Do Employees Keep Ignoring Workplace Cybersecurity Rules?

People are able to justify their bad behavior with rationalizations. Companies need to tackle the lies we tell ourselves head on.

By Anthony Vance and Zeynep Sahin

Sept. 26, 2023 12:00 pm ET

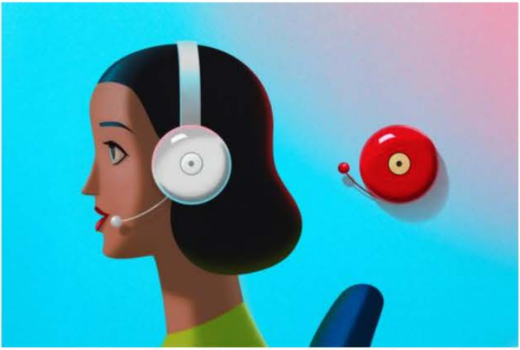
Share Resize 37 Listen (2 min)

veeAM

The threat is real.
The solution is Veeam.

Don't trust your ransomware strategy to anyone but the global market leader.

LEARN MORE



A Gartner study found that 69% of employees had bypassed their organization's security policies in the past 12 months. ILLUSTRATION: JON KRAUSE

Companies spend a lot of time making sure employees know the rules regarding cybersecurity. They cajole, they beg, they threaten. They make them take classes, sign forms, watch videos.

And yet, somehow, it does little good.

A study by Gartner last year found that 69% of employees had bypassed their organization's security policies in the past 12 months, and 74% said they would be willing to do so if it helped them or their team accomplish a business objective. All this even though most of them probably know that human error is often a factor in cybersecurity breaches.

Such indifference inevitably raises the question: Why? Why do people ignore security guidelines, even in the face of stiff penalties? Why do they flout the rules, even though they know it isn't good for either their employers or themselves?

The answer may be what criminologists have long called "neutralization techniques"—rationalizations that people instinctively use to "neutralize" the wrongness or harm of an action. Cybersecurity researchers have shown that such techniques also play a big role in employees' willingness to ignore their employer's cybersecurity guidelines.

The lies we tell

The concept of neutralization was developed by American criminologists Gresham Sykes and David Matza in the 1950s to explain the ability of juvenile offenders to "neutralize" guilt associated with misbehavior. They identified several neutralization techniques, and set the groundwork for criminologists to add techniques later on.

Typical rationalizations employees use to flout an employer's security rules include the following. Many will no doubt sound familiar, but they all have the same thing in common: They allow people to shirk the guilt they would normally feel for violating security guidelines. In this way, employees can maintain their rule-abiding self-image while drifting in and out of compliance.

Denial of injury is when employees convince themselves that no harm will come from ignoring a security policy, so breaking the rule is acceptable. And because it is acceptable, no punishment is deserved.

Appeal to higher loyalties is when employees place the demands of a work project or manager above compliance with a security guideline. They know that ignoring the policy is wrong, but they make loyalty to someone or something an imperative that overrides that.

Denial of responsibility is when employees refuse to take personal responsibility for their actions, rationalizing that the situation is beyond their control. They might claim they weren't aware of a specific security policy or weren't given the proper training to implement it.

Metaphor of the ledger is a technique in which employees mentally tally all of the positive things they do, such as working overtime or meeting quotas, and compare those to their occasional negative behaviors. If the positive actions outnumber the negative, they tell themselves they should be able to break a security rule occasionally without feeling guilty.

Defense of necessity is when employees convince themselves they were forced to behave a certain way in a given situation, so it isn't their fault. For example, they justify downloading unauthorized software from the internet because they need it to meet a tight deadline.

JOURNAL REPORTS

College Rankings
Energy
Health Care
Investing Monthly
Leadership
Retirement
Small Business
Technology
Wealth Management

MOST POPULAR NEWS

1. Americans Are Still Spending Like There's No Tomorrow

2. Gaetz Launches Bid to Oust McCarthy as Speaker

3. Rivian's Quest to Build the Ultimate Truck Burns Through Billions

4. The Secret Behind the First $1 Billion Green Hydrogen Startup

Condemnation of the condemners involves criticizing those who implement and enforce security policies and using that as justification for ignoring the rules. For example, employees might believe that the security team is unreasonable or out of touch with the needs of the business, so they view their policies as invalid and acceptable to ignore.

What can management do?

One would think the threat of sanctions would cause employees to think twice before violating a company's information-security rules. Unfortunately, sanctions for wrongdoing are precisely what neutralization techniques are so effective at dismissing. If someone convinces themselves that violating a policy isn't wrong in their circumstance, why would they fear being apprehended or punished?

But if sanctions don't work, what does?

First, security teams can use training courses to address neutralization techniques head-on by explaining their use and why they are invalid. Since so many of these techniques are second nature, bringing them to the surface makes people examine them in a way they didn't have to before.

In a study, security training was experimentally given to 87 employees of a large multinational company. Of those employees, 21 received the standard security training and 66 received training that also addressed specific neutralization techniques.

For example, the trainer described how people commonly use a "defense of necessity" to justify choosing weak passwords, believing that strong passwords are too onerous to use. Then the trainer discussed why this notion isn't necessarily true and demonstrated practical ways to choose passwords that are both strong and usable. In another example, the trainer explained how people use the "denial of injury" technique to rationalize no harm is done in using a weak password. The trainer then showed why this view is false by demonstrating how easily hackers can guess weak passwords and the damage that can be done with this access.

Employees in this latter group reported substantially higher intention to comply with the security policy in the future and lower agreement with neutralization techniques compared with those in the control group. These differences held three weeks later in a follow-up survey.

Get the message

Second, if holding a training course isn't practical or feasible, organizations can call out neutralization techniques in messages sent to employees. In one study, 200 working professionals were presented with hypothetical scenarios in which an individual used either a "defense of necessity" or "denial of injury" rationalization to violate a security policy. They were then asked the likelihood that they would behave the same way in a similar situation. Half of the scenarios included a message that directly undermined the specific neutralization techniques used, such as: "Even though people believe that sharing passwords can be justified under certain circumstances without any real consequences, adherence to this policy is important; sharing of passwords should not be justified for any reason."

5. Trump Goes to Court for Opening of Civil Fraud Trial

MOST POPULAR OPINION

1. Opinion: Matt Gaetz: 'Biden's Favorite Republican'

2. Opinion: Donald Trump's Fraud Trial in New York

3. Opinion: AOC Redefines the Term 'Rich'

4. Opinion: Jamaal Bowman and Matt Gaetz Are Alarmingly Similar

5. Opinion: High Noon for the CFPB at the Supreme Court

RECOMMENDED VIDEOS

1. Watch: Former President Trump Arrives for New York Civil-Fraud Trial

2. Matt Gaetz Plans Vote to Oust McCarthy After Speaker Avoids Shutdown

3. 'We'll Destroy You': Ukraine's Battle to Retake a Village Near Bakhmut

4. WSJ Opinion: The Second Republican Debate: Any Winners?

5. Inside Rivian and Ford's Plants, as They Race to Build EVs Faster

Advertisement - Scroll to Continue

The results showed that those who received messages that directly undermined specific neutralization techniques reported far lower likelihood that they would violate the security policy if in the same situation in the future. This suggests that simply being aware of the fallacies underlying neutralization techniques can help to reduce their use.

The key takeaway from these studies is that organizations need to understand that neutralization comes naturally to people, and no amount of threatening and insisting will change that. But management can help employees to recognize and reject rationalizations, and see cybersecurity policies for the essential role they play.

***Anthony Vance** is the Lenz Professor and Commonwealth Cyber Initiative Fellow in the department of Business Information Technology at Virginia Tech's Pamplin College of Business. **Zeynep Sahin** is a Ph.D. student at Virginia Tech specializing in cybersecurity workforce issues. They can be reached at reports@wsj.com.*

Cybersecurity

READ THE FULL REPORT

Your Online Account May Have Been Breached? Don't Just Sit There. Do Something.

Why Do Employees Keep Ignoring Workplace Cybersecurity Rules?

How to Make It Easier for Consumers to Control the Ads They See Online

10 Questions to Ask Yourself About Data Breaches

Should AI Surveillance Be Restricted? WSJ Readers Share Their Thoughts

How Much Cybersecurity Expertise Do Boards Really Have?

Your Personal Data Has Been Stolen. Will It Really Cost You Anything?

Should Software Companies Be Held Liable for Security Flaws?

Appeared in the September 28, 2023, print edition as 'Why Employees Keep Ignoring Workplace Cybersecurity Rules'.

SHOW CONVERSATION (37)

Next in Journal Reports: Technology

JOURNAL REPORTS: TECHNOLOGY

How to Make It Easier for Consumers to Control the Ads They See Online

By Suman Bhattacharyya

September 26, 2023 at 2:00 PM ET

Designing websites so controls are more visible can make the sites more cluttered looking, but may be worth it, researchers say

---

More Journal Reports: Technology Articles

JOURNAL REPORTS: TECHNOLOGY

Your Online Account May Have Been Breached? Don't Just Sit There. Do Something.

By Rajendran Murthy

September 25, 2023 at 5:19 PM ET

JOURNAL REPORTS: TECHNOLOGY

Should AI Surveillance Be Restricted? WSJ Readers Share Their Thoughts

By Demetria Gallegos

September 25, 2023 at 3:00 PM ET

JOURNAL REPORTS: TECHNOLOGY

How Much Cybersecurity Expertise Do Boards Really Have?

By Rob Sloan

September 24, 2023 at 4:00 PM ET

VIEW ALL

What to Read Next

SPONSORED OFFERS

GOPRO:
GoPro Promo Code: 15% off Next Order w/ Email Sign-up

SAMSUNG:
Samsung promo code for up to 40% Off + Free shipping

DELL:
Dell Coupon Code grab 10% off

NEWEGG:
10% off Sitewide - Newegg promo code

KITCHENAID:
KitchenAid: Up to $25 Off Artisan Series Tilt-Head Stand Mixer

GAMESTOP:
Take 10% Off military Discount - GameStop Promo Code

BACK TO TOP ^

WSJ Membership

- Buy Side Exclusives
- Subscription Options
- Why Subscribe?
- Corporate Subscriptions
- WSJ Higher Education Program
- WSJ High School Program
- Public Library Program
- WSJ Live
- Commercial Partnerships

Customer Service

- Customer Center
- Contact Us
- Cancel My Subscription

Tools & Features

- Newsletters & Alerts
- Guides
- Topics
- My News
- RSS Feeds
- Video Center
- Watchlist
- Podcasts
- Visual Stories

Ads

- Advertise
- Commercial Real Estate Ads
- Place a Classified Ad
- Sell Your Business
- Sell Your Home
- Recruitment & Career Ads
- Coupons
- Digital Self Service

More

- About Us
- Content Partnerships
- Corrections
- Jobs at WSJ
- News Archive
- Register for Free
- Reprints & Licensing
- Buy Issues
- WSJ Shop

GET IT ON Google Play | Download on the App Store

Dow Jones Products Barron's | BigCharts | Dow Jones Newswires | Factiva | Financial News | Mansion Global | MarketWatch | Risk & Compliance | Buy Side from WSJ | WSJ Pro | WSJ Video | WSJ Wine

Privacy Notice | Cookie Notice | Do Not Sell or Share My Personal Information | Limit the Use of My Sensitive Personal Information | Copyright Policy | Data Policy

Subscriber Agreement & Terms of Use | Your Ad Choices | Accessibility

Copyright ©2023 Dow Jones & Company, Inc. All Rights Reserved.