virtru

The Empowered Employee

How to Positively Govern & Influence Security Behavior in a Zero Trust World

Table of Contents

We're All Human

We've all made mistakes when it comes to security—whether that's accidentally hitting "Reply All," mistakenly sending a report to Sarah in sales instead of Sarah in human resources, absentmindedly clicking on a questionable link, or quickly forwarding an email that turned out to contain sensitive information farther down the thread.

A productive, successful, collaborative workplace requires employees to share information quickly and efficiently—but that information is often sensitive in nature. Employees need to be equipped to protect that data.

Whether it's an HR team negotiating the terms of a new benefits plan,

A marketing team preparing materials for an upcoming board presentation,

An IT consultant preparing an approach to a unique problem,

A healthcare provider sharing test results with a patient,

A lender receiving mortgage application materials from a prospective homebuyer,

A special education teacher sharing a student's individualized education plan with a parent,

Or sharing any other kind of potentially sensitive information,

It's important that your teams are empowered to share data securely and confidently.

You've heard the stats surrounding cybersecurity and data breaches—including how costly and damaging a breach can be (the average breach costs US$3.86 million[1])—and you understand why it's so urgent that companies embrace and prioritize data protection.

This guide will show you what to do about it, sharing actionable tips on how to positively, successfully empower your teams to protect their data while still being confident in their ability to share it.

1 Cost of a Data Breach, IBM

Part 1: Spark Engagement

“How do I get my employees to care about cybersecurity?”

This challenge is top of mind for technology leaders across industries, particularly those who have large workforces with a large surface area of risk. The larger the workforce—and the more globally distributed that workforce is—the more challenging it can be to monitor and guide employee behaviors around security. With 88% of breaches caused by human error[2], this is a critical area to address.

A sea change in organizational behavior starts with evaluating your current approach and what is or isn’t working. Here are a few questions to consider:

Positioning

- Am I educating employees on how data protection impacts their lives, both at work and at home?
- Am I leading with a message of fear and negativity, or one that empowers them to act with confidence?
- Am I demonstrating the benefits of good security, or just highlighting the scary consequences of a breach?
- Am I showing my employees that I trust them?
- Am I initiating meaningful dialogue or simply directing employees to a training resource?

Employee Experience

- Do my employees understand their data protection responsibility?
- Are my employees encouraged to self-report if they make a mistake?
- Am I incorporating teaching moments often to keep security top of mind, or just requiring training at certain intervals in the year?

Leadership

- Do managers at my company practice good security habits themselves?
- Do employees across the company have an opportunity to contribute to our security strategy?
- Am I giving a voice to others on my team who can share their experiences?
- Ultimately, am I giving employees all the tools they need to collaborate securely and protect data, every day?

2 The Psychology of Human Error, Tessian

To get your employees to care about security, it's important to lead with positivity and enthusiasm for the important work you do. *Show them why they should care, and what's in it for them.*

Have you ever watched someone in a niche field speak passionately about their subject matter? It doesn't matter what the topic is: marine biology, Kubernetes, tomato gardening, or their favorite band. When the speaker is visibly engaged and excited about the topic, it's compelling to listeners, regardless of how much knowledge those listeners have on the subject.

If storytelling isn't your forte, start by just sharing what you know in a positive way. Explain to employees how quickly the security landscape is evolving—both in the workplace as well as personal contexts. Talk about data privacy and emerging technology. Show them what kinds of threats you and your team have mitigated. Demonstrate how impactful their security-minded actions are.

Ultimately, strong security leads to more confidence and more freedom. Regardless of your role in a company, that's something to get excited about.

CASE STUDY

Equipping Employees to Make the Right Decisions

The philosophy of continuous learning and lifelong education is reflected both externally and internally at the Chartered Management Institute (CMI). Information Security Manager Leroy Cunningham's team uses Virtru's configurable Data Loss Prevention (DLP) rules to encrypt some types of data by default—such as credit card information—but for some categories, Cunningham prefers to issue a warning, using that as a teaching moment.

"While Virtru provides us with a safety net, we also like the idea of being able to educate our users at the same time. So, instead of automatically encrypting something sensitive, we can let the users know and advise them to encrypt it. That way, there's always a learning process in place. I think that's key: keeping security top of mind and not creating complacency. It just reaffirms that thought process and, over time, it becomes second nature to them... These aren't things that I can just teach them, it has to be something they can see and touch for themselves."

"Culture change is tough, and people are used to doing things the way they've always done it. We try to create an educational shift, so if there's anything that allows me to empower employees, and at the same time educate them, it's win-win."

Read Virtru's CMI Case Study

virtru

CMI Chartered Management Institute

"While Virtru provides us with a safety net, we also like the idea of being able to educate our users at the same time. So, instead of automatically encrypting something sensitive, we can let the users know and advise them to encrypt it. That way, there's always a learning process in place. I think that's key: keeping security top of mind and not creating complacency."

I (Zero) Trust You

Your employees and colleagues want to be treated as smart, capable, good-decision makers. When approaching security, it's important to lead by showing employees that you trust them, and that you want to give them the tools they need to be successful.

So, how can tech leaders treat their employees with trust while maintaining the necessary skepticism of a Zero Trust framework?

The idea behind Zero Trust is "never trust, always verify." That applies to all traffic—users and systems—all the time. At Virtru, we believe in a Zero Trust framework because it's a strong approach to cybersecurity, and it requires pairing data protection with strong, federated identity management.

Zero Trust treats every user and every system with equal caution. Everyone is on the same playing field. And just because your security framework requires authentication doesn't mean that you, as an individual, don't trust your colleagues.

You can trust your colleagues to do the right thing while also putting a safety net in place. When you ride as a passenger in a car, you wear your seatbelt—not because you don't trust the driver, but because there are so many variables that could cause an accident. And you want to be safe if an accident occurs.

With a Zero Trust foundation, you're doing your employees a favor. You're all on the same team, working to ensure your company's most vital assets remain secure, and a Zero Trust framework enables just that.

How to build employee trust in a Zero Trust security environment:

1. **Make security a collaborative, cross-functional process.** Not only will this spark engagement among employees inclined toward technology and data security, but it will also give you advocates across the organization. With engagement and buy-in from HR, sales, marketing, finance, product development, customer success, and other functions, you're building a network that can educate, build trust, answer questions, and influence employee behavior.

2. **Create a regular cadence of communication and feedback.** You want to keep security top of mind all year long, not just when you conduct your annual security awareness training. Additionally, If your employees are frustrated or confused about security, you want to know about it (so they don't go rogue and circumvent the processes you've put in place). Schedule technology check-ins with various teams, and/or reach out two to three times a year to solicit input, feedback, or survey data about data protection from your entire organization.

3. **Share knowledge.** Educate about best practices without talking down to your employees. Assume they're working with a limited knowledge of data security, but speak to them like the educated adults they are. They can absorb complex information and get up to speed quickly, so don't be afraid to give them some new information that might surprise them.

4. **Recognize good behavior.** Show employees just how important their actions are, and how much you appreciate them making good security decisions. If you're using Virtru, you can easily check for "power users" securing the most sensitive data. Thank them for doing their part to protect your organization.

5. **Make it easy.** Put frameworks in place that set employees up for success—like email encryption and file encryption that are simple to use and integrated within your existing applications and workflows. "It's great having all the bells and whistles, but if your end users don't know how to use it, they won't use it, and it's as simple as that," said Leroy Cunningham, Information Security Manager for the Chartered Management Institute in the U.K. "I like how clean and simple Virtru's product is, it's a simple toggle switch to turn it on or off, and it gives us more autonomy."

Putting The “Fun” In “Security Fundamentals”

You might be surprised to learn that security awareness training can not only be informative, but also enjoyable.

KnowBe4 takes it a step further: Their security training is not just well-produced—it’s binge-worthy. (In fact, their training has a cult following at Virtru, where new seasons of KnowBe4’s *The Inside Man* are met with a level of anticipation that rivals HBO’s *Game of Thrones* at its peak.)

We sat down with Roger Grimes, Data Driven Defense Evangelist at KnowBe4 and author of *A Data-Driven Computer Defense*, to understand how KnowBe4 approaches security education and behavior change.

“It’s all about culture—making it muscle memory,” Grimes said. “For a long time, American cars had seat belts, but nobody used them. Eventually, there was a culture change, and now, most people put on their seat belt the minute they get in their car. And if they don’t, the car will remind them!

“If you’re able to change the culture, you’re more likely to make people care, and make decisions to change their security behavior for themselves and for the safety of the company.”

Now It's Personal

"People may be aware but not care," Grimes said. "Until you make it personal to them, they may not follow through with the actions they've been taught."

By highlighting the risks of ransomware to employees' personal as well as professional lives, security teams can convey the consequences of cyber attacks in a more tangible way. "Many times, ransomware attacks don't just attack the company: They also attack the employee," said Grimes. "The average ransomware product is in a company for 200 days, and during that time, it's collecting all the passwords of employees. So if you go to Amazon to order something, log into your bank account to check your 401(k), access your healthcare accounts—they're getting all those passwords. So, not only can it hurt the company, but it can also infect your computer at home and cause you financial problems."

The downstream impacts of these attacks can also hurt a business from a productivity perspective. "If you and I get financially compromised while we're dealing with that mess, we're not being as productive as we could be. Plus, if your company has been financially harmed by a ransomware attack, employees probably won't be getting their bonuses that year.

"They're going to care about their personal financials even more than your company's financials," Grimes said. "You have to make people care on both sides."

Streamline Security Efforts

It's true that the cybersecurity landscape is evolving rapidly, and that cyber attacks are escalating. The World Economic Forum estimates that cyber attacks increased 238% globally between February and April 2020 alone[3]. But Grimes has good news for security leaders who may feel overwhelmed by this ever-changing environment.

"The top ways people are being compromised today have been the same for 30 years: Social engineering and unpatched software. If you want to add to that, use strong passwords and don't reuse your passwords. Those two things encompass almost all of it."

This topic is a key focus in Grimes' book, *A Data-Driven Computer Defense*. "You should fight the things that are most likely to impact you," Grimes said. "Almost no company is doing that because they're inundated with compliance guidelines that are 100 pages long and list out 300 controls. Everyone is seeing threats like bubbles in a glass of champagne, and they're not being told, 'Two of those bubbles matter more than all the other bubbles,' and because of that, they're not focusing correctly."

Simplifying your employee-facing narrative can also help solidify the most impactful behaviors you want people to adopt. For most companies, this boils down to:

- **Slow Down.** Phishing emails are becoming increasingly targeted, leveraging the terminology and lingo of even the most niche industries to appear more legitimate. As a result, phishing attacks are becoming more difficult to detect, so it's critical to slow down.
- **Think.** "Years ago, when you got a phishing email, it would come in and have all kinds of typos in it, and it would be from some weird-looking email address," Grimes said. These days, they're a lot more sophisticated. If you get an unexpected request—even if it's from someone you know—and the request is asking you for something they've never asked you to do before, think twice. Especially if that action could hurt you or your company."
- **Differentiate.** Data breaches often leak user credentials, including passwords. This can be hugely damaging for people who reuse the same passwords across accounts. It's absolutely worthwhile to use long, complex and unique passwords for each of your accounts. Grimes recommends using a password manager to help generate and keep track of these passwords, so users don't have to remember them. "No matter how you do it, you need to encourage people not to reuse the same password," Grimes emphasized. "Because every second additional website you use it on, is exponentially increasing your risk."

Ultimately, social engineering leverages human psychology to elicit behavior that exposes sensitive information, so reinforcing careful, mindful behavior and awareness is key to overcoming these risks. This is what Grimes and the KnowBe4 team work to do every day: The team even has a phishing counselor on staff to examine why people make the decisions they do.

3 Why the Hybrid Workplace is a Cybersecurity Nightmare | The Wall Street Journal

Part 2: Create a Layered Security Framework

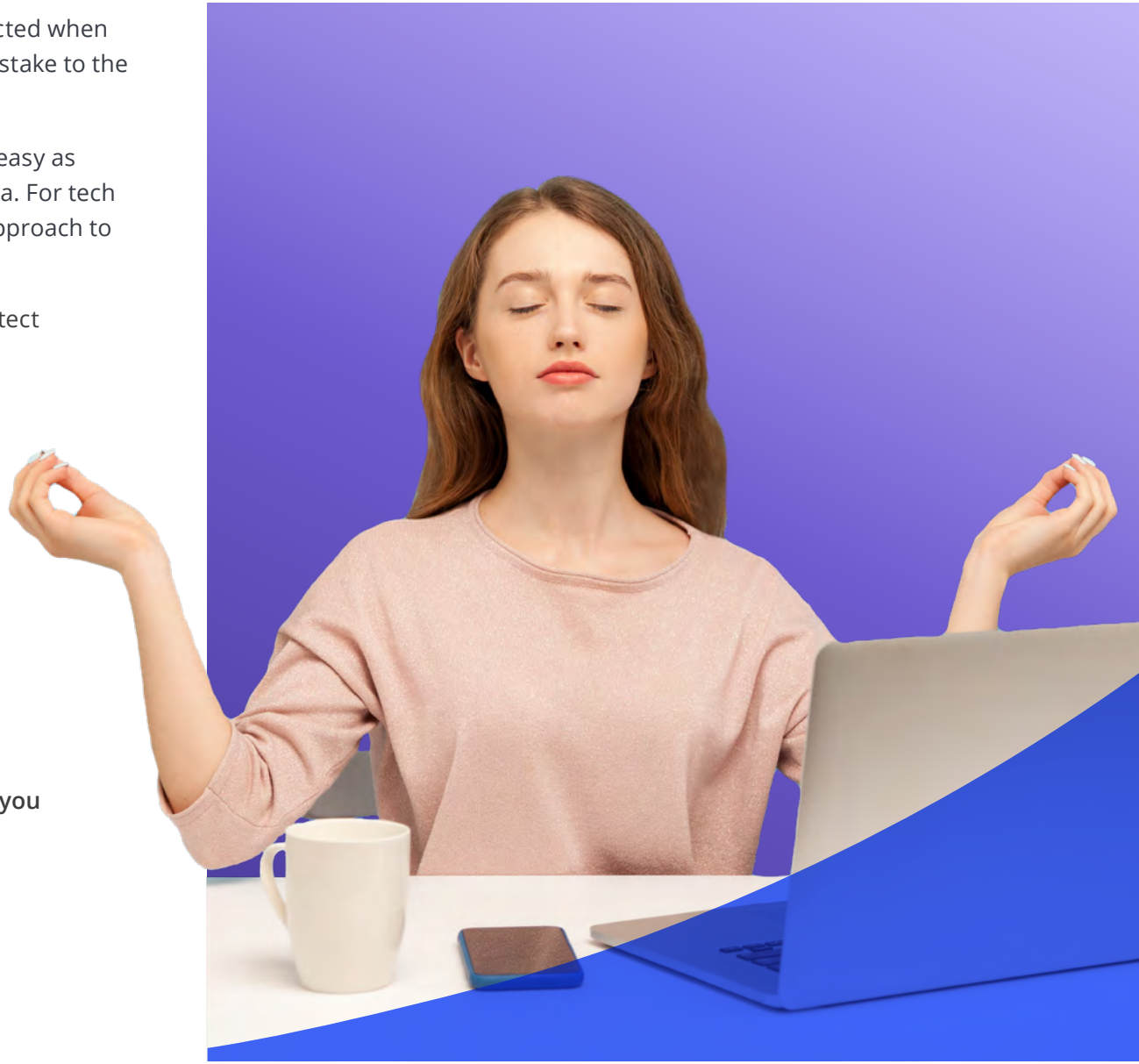
Despite our best efforts, none of us is perfect.

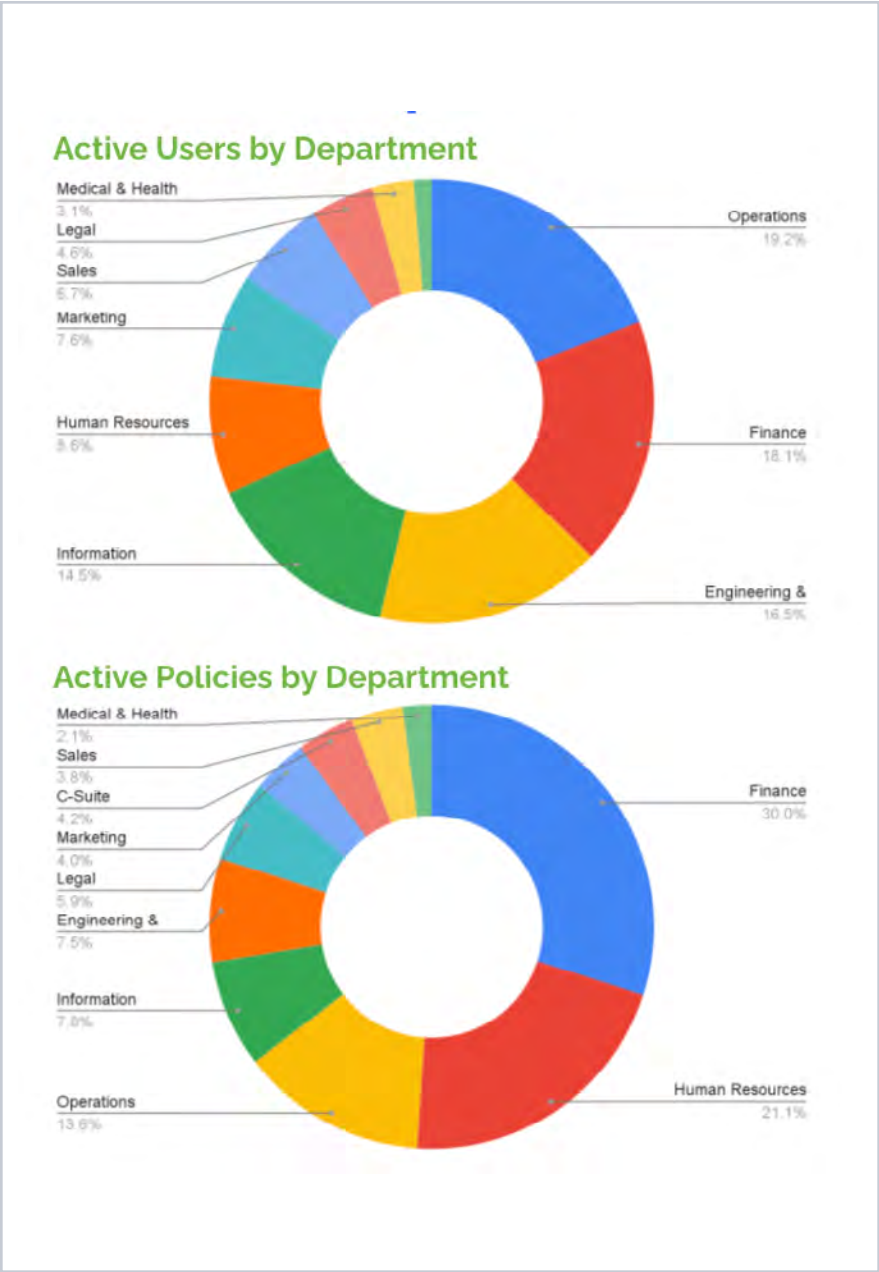
People open emails in a hurry. They might be distracted when they click on a link. They may hesitate to report a mistake to the IT team for fear of getting in trouble.

Part of empowering your employees is making it as easy as possible for them to do the right thing with their data. For tech leaders, this means implementing a multi-layered approach to security, including:

- Easy-to-use tools that empower employees to protect the information they're sharing
- Multi-factor authentication and federated identity to govern data access
- Comprehensive employee training and education
- Protecting data at the object level so that it's safe everywhere it travels
- A "safety net" that mitigates human error
- Closely monitoring network traffic for anomalies

Mistakes are going to happen, but there are steps you can take to mitigate them.





Adopt Security That Travels With The Data

The average employee sends over 10,000 emails every year.

Do some quick math and multiply that by the number of employees at your company (or use Virtru's Data Sharing Calculator). That's a lot of data being shared.

If you have no visibility into where those emails are going—how often they're being forwarded, where the attachments are ultimately being shared—that surface area of risk is not just large: It's largely unknown.

According to a recent Virtru study, finance, HR, and operations (which includes customer support) departments accounted for nearly two-thirds of the sensitive data being shared. These departments can be considered "super-users" of data protection. Other teams, including the C-suite, sales, legal, and engineering teams, also shared a considerable amount of sensitive information.

Organizations today need to share data in order to collaborate and innovate, across every department, and every level of an organization. So, how can technology leaders gain more confidence and visibility into how that data is created, shared, and stored?

If you implement a data-centric security strategy that protects data with object-level encryption it will essentially wrap each file or message with its own distinct layer of protection, making data sharing far more manageable.

Another benefit of data-centric security is that it protects the data itself, everywhere it travels, leaving you with greater flexibility for the future. This is instrumental in setting yourself up for success in a security landscape that evolves so rapidly. By protecting the data itself—everywhere it travels—you have the flexibility to adopt new tools and vendors, equipping your employees with the collaboration and data-sharing tools they want to use.

With data-centric methodologies, you can be confident that your strategy is sustainable for the future. With this mindset, you'll choose vendors and partners that align with your approach and can provide you with full control over your own data, everywhere it goes.

"Privacy is a human right, and people shouldn't have to sacrifice security or ownership when they share their data."

"My brother and I started Virtru nearly a decade ago, with the objective to make data protection accessible to everyone," said Will Ackerly, Virtru's Co-Founder, CTO, and inventor of the Trusted Data Format (TDF). "Privacy is a human right, and people shouldn't have to sacrifice security or ownership when they share their data. Nine years later, Virtru's offerings are deployed across 6,000 customers, from small businesses to large global enterprises, while remaining free for individual, personal use. That privacy mission continues to drive our innovation, and we use the TDF to protect all kinds of data: Not just email and files, but data that is relayed from low-bandwidth, edge IoT devices in challenging environments."

With Virtru's email encryption solutions for Gmail and Outlook, employees can easily share sensitive data and determine how they want to secure that data, whether they want to allow forwarding, expire messages after a certain date, or even revoke an email when needed.

Eliminate Unnecessary Friction

Generally, employees need to make some kind of tradeoff between convenience and security. Authenticating their identity for multi-factor authentication adds a step to the log-in process. Encrypting an email adds an additional step to sending. Slowing down and taking a moment to examine a suspicious email takes some conscious effort.

The key to get employees to adopt your security recommendations and tools is to make them truly simple, seamless, and easy to use. Wherever possible, remove friction from your employees' security experience and reduce the "inconvenience tradeoff" they make for various aspects of your security tech stack.

Ask yourself:

- How can I free up my employees to do their jobs to the best of their ability?
- Where can I remove friction to enable them to communicate and innovate more seamlessly?
- Which legacy tools and products are no longer meeting our needs? (Or aren't evolving rapidly enough to keep pace with my organization?)
- How can I surprise my team with easy-to-use solutions?

For your employees to actually use the security tools you provide, they must be easy for both your internal *and* external users to adopt. Look for solutions that are integrated natively within both Gmail and Microsoft Outlook, so that users can easily encrypt emails and set access controls with the flip of a switch. In addition, look for solutions that allow the recipients to easily verify their identity so they can access emails without the need for creating separate credentials.

> With security products, you always have to worry about user adoption, but Virtru is so easy to use that this hasn't been an issue. After all, security and compliance aren't about the technologies you buy, they're about the products that are actually used."
>
> -Mark Dieterich, CISO, Brown University
>
> Read Virtru's Brown University Case Study

That end-user experience is critical to consider. Your executive team, customer success teams, and sales teams place high value on making a good impression, and they want to put their best foot forward. If they know your encryption tools are going to be clunky or create hurdles for their customers, they probably won't use them.

But if you adopt a solution that empowers your employees with ease of use and security, it's a win-win.

Construct A Safety Net For Human Error

In a perfect world, your employees would continually operate with security in mind, making the best decisions to protect their data, every time.

But we don't live in a perfect world, and that's OK. We can still create a safety net for when employees don't make the right decisions.

Data Loss Prevention (DLP) rules can be put in place as a safety net to catch emails and files that employees either intentionally or unintentionally fail to encrypt. Administrators can set and customize DLP rules to automatically encrypt messages containing certain types of sensitive information.

For healthcare providers, this could include protected health information (PHI)—including medical records and test results—or things like billing information and other PII (personally identifiable information). For financial services, it may be tax forms and payroll data. For educational institutions, it could include individualized education plans (IEPs) or student health data subject to HIPAA.

Look for solutions that allow you to choose how to put certain DLP rules in motion: Equip your organization to automatically encrypt certain types of data, or warn users when potentially sensitive information is detected in an email. For example, an organization could choose to always encrypt emails containing a social security number, but in cases of an address or phone number being shared, they could issue a warning to the sender and allow them to make the final decision. Based on data from Virtru, when users receive a warning, 22% of them decide to encrypt the message they're sending.

That reminder can be a useful nudge to get employees to think about securing their data, so many administrators use it as an educational opportunity. "While Virtru provides us with a safety net, we also like the idea of being able to educate our users at the same time," said the Chartered Management Institute's Leroy Cunningham. "So, instead of automatically encrypting something sensitive, we can let the users know and advise them to encrypt it. That way, there's always a learning process in place. I think that's key: keeping security top of mind and not creating complacency. It just reaffirms that thought process and, over time, it becomes second nature to them... These aren't things that I can just teach them, it has to be something they can see and touch for themselves."

There are some types of data that should always be encrypted, regardless of the circumstance. By putting DLP rules in place, you can empower your employees to collaborate as needed with the confidence that your most vital data will always be protected.

Give Employees Autonomy

Sometimes, data sharing isn't black and white. Data sensitivity is nuanced, and each situation may call for its own parameters for sharing data.

Virtru puts sophisticated controls into the hands of the end user, giving them options for setting parameters around how their data can be used. They can disable forwarding, add watermarks to attachments, or set an expiration date for information they share.

Perhaps the most powerful tool Virtru provides is the ability to revoke access to files or messages at any time. If a third-party vendor experiences a breach, or a certain file was inadvertently shared, or the user mistakenly hit "Reply All," they can immediately revoke access, even if that file has already been viewed by the recipient.

This also gives the employee an opportunity to correct their own mistakes. Rather than hoping their data doesn't end up in the wrong hands, they can take control immediately, at any time.

Now that's empowerment.

Part 3: Inspire Action

Now that you've sparked the interest of employees and put a strong security framework in place to support them, how do you put all this into motion and start influencing behavior across your organization?

The key is to make security a habit, an everyday part of your organization's life. Just like any other habit, it's about small, continuous shifts that add up to a big impact.

As a security leader, the tools and communications you introduce can help facilitate a behavioral shift and gently remind employees to be mindful of security in a fast-paced workplace.

Shift Employee Behavior

In 2020 alone, Virtru users created over 68 million secure data-sharing policies (emails and files): That's a lot of data that may have otherwise been sent unprotected. Of those 68 million data assets, 13.7 million were encrypted automatically through Virtru's Data Protection Gateway, which encrypts data flowing through enterprise SaaS applications like Salesforce, Zendesk, and Looker. The remaining 54.3 million were encrypted either individually by users within Gmail or Outlook, or automatically encrypted using DLP rules set by the administrators.

This creates a blend of automated safety-net data protection and voluntary, opt-in data protection that employees decide to apply.

Use the tools at your disposal to put positive, security-focused messages in front of your teams. Here are a few ideas:

- Leverage Virtru's warning feature, mentioned above, to alert employees about certain types of sensitive data they're sharing.
- Highlight the "security heroes" of your organization on a monthly or quarterly basis, whether it's someone on your business technology team or an end user that's doing a great job protecting the organization's sensitive data. This can be a chance to highlight and recognize positive behaviors like reporting suspected phishing or aligning with your team on a certain type of data that needs to be better protected.
- Share your team's wins, whether it's applying a critical patch, developing new workflows, or modernizing part of your technology stack. Use this as an opportunity to educate the enterprise about the important work being done in your department, so they don't take it for granted.

Bridge The Gap Between Work And Home

Large-scale data breaches are in the news with increasing frequency, and with increasing magnitude. Incidents impacting large enterprises quickly become big headlines, with various ransomware and data breach incidents coming to light at a steady pace.

Use these incidents as an opportunity to educate and engage. Help your employees understand what these breaches mean, what happened, and what they can do to help your organization remain secure in an increasingly sophisticated and challenging threat landscape. Show them the kinds of threats to watch out for, and remind them of the importance of each individual's actions.

Additionally, demonstrate how best practices at work can translate to best practices at home. No one wants to have their identity stolen. No one wants to see their bank account suddenly emptied. Show employees that the consequences of ransomware, weak passwords, and unsecured data sharing can have a big impact on their own personal life, as well as the future of the company.

This should help put security into perspective and demonstrate that it's not just the IT team's job, and it's not just something to be mindful of at work. It should be part of every interaction with technology—from computers to phones and IoT devices—both at work and at home.

Ideas for Sparking Conversations Around Security

- Explain Data Breaches in the News
- Provide Tips for Managing Tech at Home and at Work
- Answer Employee Questions about Security-Related Concepts
- Demonstrate the Power of Each Individual's Actions
- Connect the Dots Between a Workplace Cyber Attack and Individuals' Personal Accounts and Data

Create Advocacy Internally

Once you've cultivated employee engagement around the subject of security, harness that power and maintain it. An employee who advocates for strong security practices can not only make a positive impact, they can provide you with recommendations based on their day-to-day observations. If certain platforms are too clunky to use, or if people are growing weary of certain security messaging, they can let you know.

Take note of the people who ask the most questions about security best practices. Keep an eye on your Virtru Control Center to see who your "super users" are, and understand what makes encryption so valuable to them. You'll start to find advocates across your enterprise who can positively influence behavior while also giving you honest feedback from their own teams.

Conclusion

At the end of the day, a core pillar of managing security is managing people—and like any exercise in leadership, governing employee behavior requires clear communication, fostering engagement, and creating connection.

By equipping employees with easy-to-use tools, compelling education, and a security-minded company culture, you can set your organization up for success. Even as the threat landscape evolves, you'll have an engaged security defense that spans your entire organization.

Here's to your engaged, empowered, and energized team!

About Virtru

At Virtru, we empower organizations to unlock the power of data while maintaining control, everywhere it's stored and shared. Our portfolio of encryption solutions and tools—built on our open data protection platform—governs data throughout its lifecycle. More than 6,000 customers trust Virtru for data security and privacy protection.

To learn more about how we can help you empower your team with user-friendly, data-centric security, contact Virtru to start the conversation.