Smash 3 Cybersecurity Myths to Improve Employees’ Behavior

by Phillip Shattan

Employees flouting cybersecurity rules is an intractable problem in the workplace — and it’s an issue that’s not going away. The reason: People make the wrong assumptions about how they should behave, which makes lax habits much harder to shift. In a digital business, functional leaders must get this right and bust the most pervasive myths.

Half of employees regularly engage in unsecure behaviors online, such as sharing their password with a co-worker who shouldn’t have access or clicking on a link from an unknown source and exposing the organization to a malware attack. Eighty-two percent of incidents in the workplace are caused by human behavior, according to the U.S. telecommunications company Verizon.1

People make the wrong assumptions about how they should behave, which makes lax habits much harder to shift.

What these stark numbers reveal is that it doesn’t matter how much money your organization spends on cybersecurity if employees don’t prioritize it. And functional leaders who try to enforce more secure behavior by shining the spotlight on security awareness, or through good “tone at the top” conduct, are likely doing little to improve the situation.

Root Causes of Unsecure Cyber Behavior at the Workplace

Unfortunately, employees’ cybersecurity practices are often reinforced by assumptions that make them harder to correct (see Figure 1).

How to Fix Flawed Assumptions

Changing this sad state of affairs requires a reset in how CISOs and their colleagues throughout the enterprise think about cybersecurity rules (see Figure 2). And it starts with three steps, each of which flows from correcting a flawed assumption:
• Reduce the burden employees experience from the number of cybersecurity policies they have to navigate.

• Increase accountability throughout the business, including getting functional leaders to do the right thing.

• Teach employees how to take acceptable risks. Sometimes it is justifiable to violate certain, though not all, security policies.

### Figure 1. Underlying Assumptions and Root Causes

<table>
<thead>
<tr>
<th>Underlying Assumptions</th>
<th>Root Causes</th>
</tr>
</thead>
</table>
| Employees feel weighed down by their organizations’ cybersecurity expectations and often ignore them for the sake of immediacy. | • Increased speed or convenience is the top reason employees behave unsecurely.  
• One out of every three used unapproved USBs to get work done more quickly, knowing full well the risk to the company network. |
| Employees aren’t held accountable.                          | • On average, nearly one-fifth (18.5%) of employees said the main reason they violated the rules was because they wouldn’t face any consequences for doing so.2  
• Shockingly, 70% believe there will be no consequences to bypassing their enterprises’ cybersecurity guidance. Without accountability, your workforce will never prioritize security. |
| It’s OK to sometimes violate certain policies, but employees don’t know when. | • Certain behaviors present more risks than others, but people don’t know which rules are more important, especially if some seem arbitrary or irrelevant.  
• Nearly one-third of employees believe security policies are hard to understand, inflexible and not appropriate for their roles.  
• Alarmingly, that number jumps to almost half for business technologists (who engage in activities previously restricted to IT, such as app development). They have even more difficulty knowing which cybersecurity rules to prioritize. |

Source: Gartner
**Myth 1:** Employees act unsecurely because they aren’t aware of the risks certain behaviors cause. Functional leaders should therefore promote security awareness throughout the business.

**The Truth:** Most employees who violate security policies know not only what it is they are breaching but also that their behavior is troublesome. They just think the risk is worth it.

For example, 72% of employees who transfer sensitive corporate information between personal and work accounts know that it hikes risk, but they do it anyway for the following top three reasons:

1. It is convenient (cited by 25% of employees).
2. Business needs outweigh the risk (cited by 24% of employees).
3. They don’t believe they will face any consequences for doing so (cited by 14% of employees).

All the security awareness in the world won’t change this behavior.

**What to Do About It:** Instead of raising security awareness, tackle the added cognitive overload that security imposes on your workforce. The CISO can only do so much to reduce this business friction on its own; strong support from functional leaders is critical. They must work with the CISO to identify and lessen this burden.

**Figure 2. Corrections for Three Myths to Drive More Secure Behavior**

<table>
<thead>
<tr>
<th>Myth</th>
<th>Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>More security awareness leads more secure behavior.</td>
<td>Reduce cognitive overload.</td>
</tr>
<tr>
<td>A “good tone at the top” automatically leads to more secure behavior.</td>
<td>Back up well-meaning words with accountability.</td>
</tr>
<tr>
<td>Violating policies is always a bad thing.</td>
<td>Teach employees how to take acceptable risks.</td>
</tr>
</tbody>
</table>

Source: Gartner

To make it easier for employees to follow the rules, do at least some of the following:

- Use policy violations and exception requests to identify burdensome rules.
- Regularly revisit controls to see if they still apply. For example, if your organization recently moved to the cloud from servers located on-premises, your policies should be updated to reflect that change.
- When updating policies and controls, coordinate among security and the affected business units so they work together, rather than having the CISO updating them without input from functional leaders. Meaningful collaboration efforts can include working groups, security champions, communities of practice, feedback sessions and proofs of concept.
- If a business unit no longer needs access to certain data, have the relevant functional leader proactively tell security to restrict or even remove access. In return, some of the controls security has in place, such as the use of certain tools, can be removed.
- Have the CISO talk to employees to understand what applications and tools they want to use; when those requests can’t be fulfilled, make sure a viable alternative is available (and that employees are aware of it).
**Myth 2:** Tone at the top guarantees secure behavior.

**The Truth:** While it may be tempting to think you are doing enough to support security by voicing support, saying the right thing is the bare minimum, and it is insufficient on its own.

Two-thirds of employees say they have been praised by senior leadership for acting securely, yet over half of them admitted to violating security policies multiple times in the previous 12 months. They do this, on average, for the following top two reasons:

1. Increased speed or convenience (cited by 18% of employees)
2. Business needs outweighing the risk (cited by 29% of employees)

Even when executive messages are good, most employees still see security as a barrier or an afterthought.

**What to Do About It:** Back up your well-meaning words with accountability.

Over half of employees believe it is the cybersecurity team's job to keep the enterprise safe. A sense of fairness and set of clear expectations from leadership help employees understand it is, in fact, their responsibility, too.

**Here's how you can develop good cybersecurity behavior throughout the organization:**

- Work with security to make sure it can enforce real penalties for poor behavior. When asked what consequences would be most likely to make them change their behavior, employees chose escalating warnings and sanctions.
- Treat cybersecurity the same as other business metrics, such as project budgets and deadlines; otherwise, even employees who know it matters won’t prioritize it. If they see top performers rewarded for acting unsecurely, why should they care?
- Make managers accountable for security (and reduce friction) by giving them the ability to approve certain security exceptions. For example, employees who want to visit certain websites that are blocked can get signoff from their bosses.

---

**Myth 3:** Unsecure employee behavior is always a bad thing.

**The Truth:** While there are certain lax habits employees should never do, it is sometimes OK to engage in appropriate risk.

It’s clearly a problem that nearly half of employees regularly open email links and attachments from unknown sources on a work device, but roughly a quarter of them did it by accident. And the top three reasons why employees won’t self-report a policy violation are:

1. Fear of looking foolish in front of their colleagues (cited by 37% of employees)
2. Fear of reprisal or disciplinary action (cited by 33% of employees)
3. Belief that the impact of the action is insignificant (cited by 20% of employees)

Eighty-five percent of employees who regularly shared their passwords with a co-worker did so deliberately — even though the colleague did not have formal permission to use it. They understood the risk, and believed it was an appropriate one.

Some employees may not fully understand the trade-off they’re making, but over one-third claim to regularly consider the organization’s position when taking actions that could introduce cybersecurity risk. In these cases, “unsecure behavior” isn’t a bad thing; it’s a sign of mature risk decision making.

**What to Do About It:** Instead of providing rote guidance, functional leaders should make sure employees — especially those who fulfill multiple roles — have appropriate tips.

Help employees understand your organization’s risk appetite and provide tailored resources so they can make informed decisions:

- Run risk workshops, provide lists of common risks and compensating controls, and use APIs to automatically highlight risks. Offer employees several options so they can develop the ability to recognize when it’s OK to bend certain rules, and which rules need to be prioritized.
• Encourage employees to report real incidents — whether it’s a result of their own lax behavior or a breach they have witnessed — and make it clear they will not be shamed or punished for speaking up. This not only alerts security but also helps your workforce learn which behaviors create more risk.

• For newer roles, such as business technologists, don’t assume existing guidance is sufficient. Business technologists are not professional coders, and — more so than IT or regular end users — they need lots of clarity. Create jargon-free resources so nonexperts can use them.

• Review your cybersecurity policies to make sure they make sense. If they do, people will think twice before breaking them (and then, ideally, only for a good reason). But if you have a bunch of (seemingly) arbitrary policies, employees will violate them — even the important ones — without a second thought.

• Treat security exception requests as opportunities to improve policies. While some things that are frequently on the wishlist (such as access to Netflix) may be inappropriate, many exception requests reveal legitimate and constructive feedback on existing policies. If an employee wants access to a specific tool — and no viable alternative is currently available — work on procuring one, or consider whether the tool should be restricted in the first place.

Unsecure employee behavior is the No. 1 cause of breaches. But reframing the way you partner with the workforce will convert your people from a liability into the first line of defense — without your organization having to invest in a single new security tool.

2 ‘On average,’ in this case, refers to taking the responses from multiple questions and calculating the average from that, rather than the average response to a single question.
Connect With Us

Get actionable, objective insight to deliver on your mission-critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

**U.S.:** 1 855 811 7593

**International:** +44 (0) 3330 607 044

Become a Client

Access the latest edition of Gartner Business Quarterly here.

Learn more about Gartner for IT Leaders
gartner.com/en/information-technology

Stay connected to the latest insights