HackNotice

Security is a Team Sport:

How to Create a Culture of Security in Your Organization

Table of Contents

Cybersecurity is critical for establishing trust, earning new business and satisfying existing customers, protecting your brand, and keeping your company's intellectual property from landing in the wrong hands. It's critical to every aspect of your organization's future.

Unfortunately, it's also becoming much harder to manage.

Hackers can strike at any time from anywhere.

For more than two decades, IT security professionals have borne the brunt of the responsibility in defending companies against cyber threats. If a hacker infiltrates a network or sensitive data is exposed, they're the ones held accountable and forced to clean up the mess. As the most qualified experts on cybersecurity, it always made sense that they'd be charged with protecting against intruders.

There's just one problem: Today, every employee has a key to the castle. And no matter how knowledgeable, experienced, or dedicated your security team — or how robust your cybersecurity tools — all it takes is one act of employee negligence to bring your entire organization to its knees.

To mitigate the risk, modern CISOs not only have to evaluate whether they have the proper infrastructure, but also how well their security program is performing. Most importantly, they have to ensure everyone is committed to squashing threats and keeping the business safe.

That's a big job.

The good news is, using frameworks like security performance management, security leaders can determine whether employees are supporting security measures or ignoring protocol and bypassing controls to do their work faster and easier — which is a common issue with grave consequences. And by building a culture of security, they can maximize protections.

Digital defense is critical 24/7.

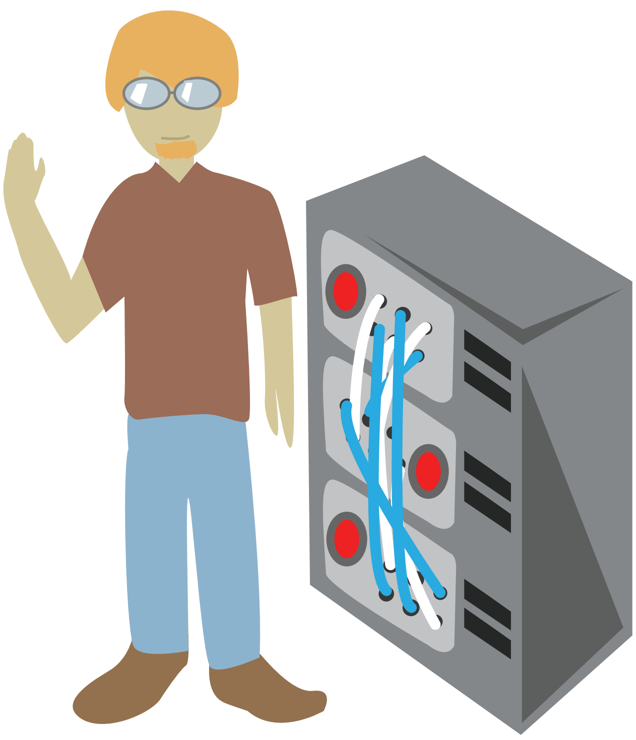
In this guide, we're delving into what it means to have a culture of security, how to break down the silos preventing you from democratizing security, how to earn buy-in from senior management, and how actionable threat intelligence can support your efforts.

The cybersecurity revolution is here, and it's up to you to lead the charge. Let's get started.

What is the Security Performance Management Framework?

Security performance management (SPM) is a method of assessing and managing your company's cybersecurity program, including how well employees use your security tools and processes. It can also help you determine the human capital and financial resources necessary to meet your cybersecurity goals in a way that maximizes both the program's effectiveness as well as its efficiency.

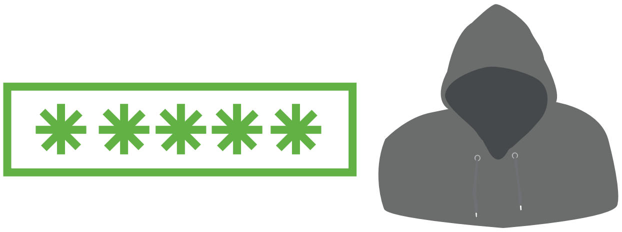
SPM is made up of two components: the infrastructure and the personnel using the infrastructure.



Expensive, high-tech cybersecurity infrastructure is only as good as the people using it.

Your infrastructure refers to all the technologies you put in place to help mitigate your risks. This includes (but isn't limited to) antivirus software, firewalls, hardware endpoint protection, and VPNs. According to data from the RSA Conference, companies spend a significant amount of money on these products — about $124 billion in 2019 alone. And it makes sense. After all, if your organization isn't secure, you could lose everything.

But no matter how much you spend on your security infrastructure, it won't do a bit of good if the people you employ aren't using it correctly. For example, you could install the best antivirus in the world, but if an employee falls for a spear-phishing scam and inadvertently gives their password to a hacker, it's all for nothing.



Instead of continually spending more and more of your budget on increasingly more sophisticated programs, it's a better use of time, money, and energy to ensure your workforce is using your existing infrastructure effectively.

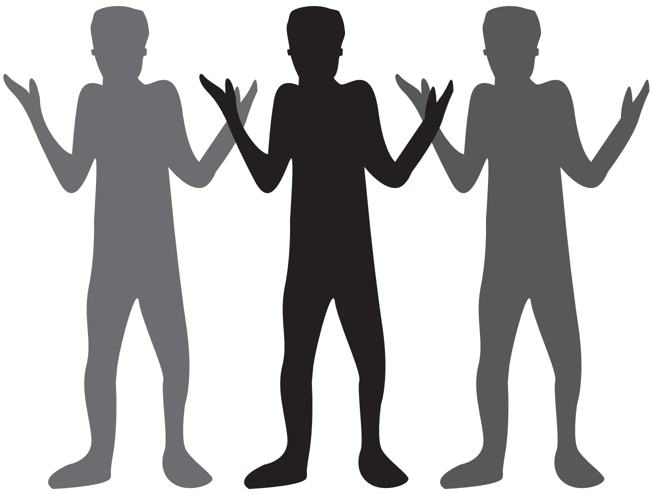
And that's where the culture of security comes in.

When everyone in the company understands their responsibility to protect against cybercrime, you can increase your security performance while potentially reducing your infrastructure expenses. Or, at the very least, making the best use of the security budget you already have.

What is a Culture of Security?

A **culture of security** is an environment in which employees not only understand the importance of strong cybersecurity, but also actively participate in protecting the organization against hacks and leaks.

Like any other values the company may uphold, security should be woven into every process and calculated into every decision. When security is part of the culture, each member of the business accepts personal responsibility for their actions online and recognizes they'll be held accountable if they choose not to comply.



Employees with poor security habits can unkowingly open up their organization to hackers.

With the advantages of working digitally come the responsibility of keeping information secure.

Here are a few examples of a powerful culture of security:

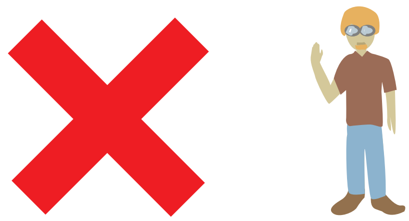
- *Employees understand the difference between a strong and weak password, and change passwords regularly without being asked.*
- *Employees know how to identify potential threats, like phishing emails, and immediately report them to the security team.*
- *Department heads always work with security leaders to vet third-parties before investing in a new service or signing a contract with a new vendor.*
- *Employees never sign up for services unrelated to business on their company devices or use corporate login credentials for personal accounts.*
- *If an employee makes a mistake, they let the security team know and take the necessary actions to correct their misstep.*
- *Employees don't share passwords, door codes, keycards, or other assets because they recognize how easily they could fall into the wrong hands.*
- *No one feels they're above cybersecurity rules, regardless of duties or seniority.*

7 Steps to Building a Culture of Security in Your Workplace

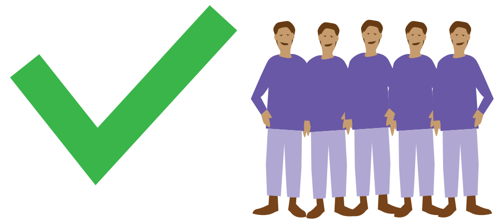
To make security foundational to your company culture, you need to democratize it.

In other words, if you want to be successful in protecting your organization, then you can't manage cybersecurity in a silo where security leaders are the only professionals with insight into how well your organization is performing. Rather than the traditional, top-down, authoritarian model of security, it must become collaborative.

After all, without visibility into your business security — or the steps security teams take to mitigate risks and clean up messes — employees will always assume everything is fine. By giving them insight into your processes, and the knowledge and skills to make their own decisions, they feel empowered to participate in the culture of security.



Silo'd security information isn't benefitial because the majority of people don't see the impact of their behaviors.



Active participation in the security process creates a team of employees who understand the importance of cybersecurity.

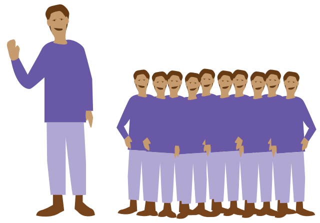
But how, exactly, can you democratize security? Here are seven steps we recommend:

Step 1: Survey your current situation

Start by assessing where you are today. Are employees actively engaged in the security process? How do you ensure they're up to date on the latest best practices? Do you alert the organization when there's a threat or attempted breach? (If so, how?)

Step 2: Educating all employees on their responsibilities

Once you've identified where your organization stands, it's time to fill in the gap. Take time to educate employees on your cybersecurity process and their role in keeping the organization safe. This would be a good time to refresh them on best practices for passwords, where to report suspicious activity, and what they can do to protect your company while online.



Step 3: Charge department heads with reinforcing security

A team is only as strong as its leader. A culture of security won't thrive unless each department leader is committed to upholding security standards. As with any other compliance requirements, department leaders are ultimately responsible for how well their team performs.

Step 4: Deploy actionable threat intelligence

One of the best ways to maximize security performance is to leverage threat intelligence technology. This way, you can identify whether your organization has been compromised, alert the company, and identify where the issue originated.

It also helps you measure your organization's progress. For example, if the number of reported hacks declines over the course of a quarter, you know your security efforts are effective.

Step 5: Hold employees accountable

When you can trace the origin of a potential hack, you can determine which individual or department is responsible. For example, you might conclude that an employee used company credentials to set up an account on an unauthorized website, or you might discover an entire department is sharing one login for a service.

This insight allows you to hold employees accountable, ensure they correct their mistakes, and foster better security habits.

Step 6: Re-educate "slackers"

Instead of forcing the entire company to sit through security education every quarter, focus on refreshing your security slackers (employees who are lax about the rules and making the sorts of mistakes your processes exist to avoid). Over time, your least security-conscious employees may become the best-informed.

Step 7: Celebrating and recognize key wins

Be sure to reward the teams and individuals who are supporting a culture of security. If a department completed a quarter without an incident, for example, recognize them with a bonus or an extra day of PTO. This will inspire their continued commitment, and incentivize slackers to improve their performance.

How to Earn Buy-In from Senior Decision-Makers

We know what you're probably thinking: "This sounds great, but my senior executives are focused on other priorities."

Today, most c-suites are more focused on achieving and sustaining growth than ensuring employees follow cybersecurity protocol. After all, education takes time, threat intelligence requires budget, and they'd likely rather spend those resources on activities that directly drive profits.

As a security leader, it's your job to show them exactly how your mission aligns with organizational goals and that, without effective cybersecurity, those other objectives may be for nothing.

Here are three things you should focus on when making a case for a culture of security:

Decision-makers need to know that everyone practicing cybersecurity benefits the entire company.

Focus on financials

The c-suite is always focused on the bottom line. CEOs and CFOs are especially concerned with maximizing profits while minimizing expenses and are usually open to any suggestions for increasing the company's operational efficiency.

At first, taking additional security measures can seem like a lofty expense — which is why you need to flip the script. It's crucial you share how boosting protection will not only help save the organization from costly hacks, but democratizing security will actually make the company money.

Today, every business is concerned with cybersecurity, and most consider this factor when evaluating potential providers and partners. A culture of security will help you stand out from the competition by showing potential clients you take it seriously. And once you've earned their trust, existing customers are less likely to churn.

Bottom line: Better security equals more revenue — the return on investment is undeniable.

Focusing budgets where every dollar is used effectively is the easiest way to save on security spend.

Identify reputational aspects

From legal fees and settlements to third-party forensics and infrastructure repair, there are lots of costs associated with a hack or breach. But perhaps the most significant cost is the damage to your organization's reputation. If the millions (or billions) of dollars spent repairing the problem doesn't send you into bankruptcy, the customers you lose in the aftermath might be the final straw.

Take Equifax, for example. In 2017, a hack exposed about 147 million Americans' personal data (including home addresses, social security numbers, birthdates), according to the Federal Trade Commission.

In the week following the announcement of the leak, the credit reporting bureau's net worth dropped more than $3.5 billion, according to Macrotrends. Years later, Equifax's reputation still hasn't recovered and most consumers can't hear the credit reporting bureau's name without thinking of its massive hack.

(Check out this blog post for three lessons we've learned from other big hacks.)

Bottom line: A major hack could irrevocably destroy your organization's reputation.

Simple security is a powerful tool when every part is used correctly and efficiently.

Company gains can quickly turn into company losses when customer data becomes compromised.

Highlight efficiencies

One of the c-suite's primary roles is to ensure efficiency across the organization — including efficient use of time, money, and employee skills. Efficiency drives productivity, which, in turn, translates into increased revenue potential.

Often, increasing efficiency means reviewing all existing products, services, and processes to ensure they're worth the investment of resources. And if your organization is like most, cybersecurity represents a pretty hefty line item.

When you cultivate a culture of security, you can ensure all the technology you're investing in to protect your company is be used to the fullest, and, in some cases, you may be able to shrink this expense. Furthermore, when everyone is doing their part to identify threats and avoid risks, IT professionals spend their time working more proactively (i.e., finding new ways to help employees work smarter) rather than reactively (i.e., cleaning up security messes).

Bottom line: When every employee participates, cybersecurity is cheaper and more effective.

How Does HackNotice Teams Help Foster a Culture of Security?

Cybersecurity isn't a technology problem — it's a people problem. And a culture of security is the solution. But, to democratize security across your organization, you need the right platform.

"HackNotice Teams gives clients the opportunity to be proactive by providing feedback about strengths and weaknesses within their cybersecurity programs, including which areas require more attention and the types of changes to work culture that can enable a more secure environment."

— Romaine Marshall, Cybersecurity, Privacy, and Business Litigation Lawyer at Stoel Rives

HackNotice Teams helps make a culture of security possible by distributing information throughout your organization, reminding employees to practice good habits, and automating data collection so your security team knows which employees need the most help. Here's how:

Spreads knowledge and responsibility

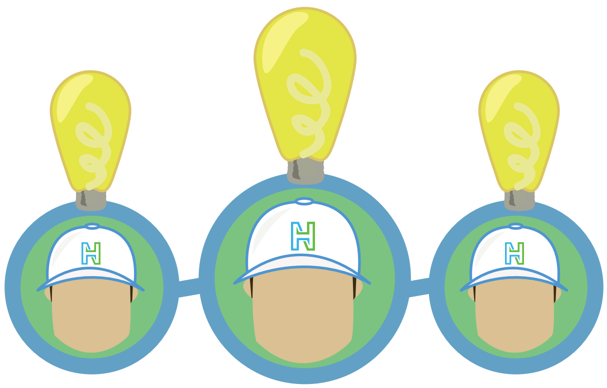
HackNotice Teams gives everyone insight into security issues — not just the CISO. When an employee's information is involved in a potential hack, they're notified immediately so they can understand where the threat originated and which steps they should take to prevent further consequences — like account takeover.

Fosters better habits

This platform helps cultivate better decision-making by not only showing employees what they can do to improve their cybersecurity habits in the future, but also urges them to correct their mistakes.

Focuses education on those who need it most

Cybersecurity education is necessary — but it's also time-consuming and can be expensive. HackNotice Teams allows you to focus your training resources only on those who need it most. Furthermore, with self-study modules, you don't have to worry about pulling security pros from their work to re-educate employees.



Hackers have limited openings into an organization when employees use basic security practices.

Identifies highest risk personnel

Who is doing the best job supporting your cybersecurity goals? And who is doing the worst? HackNotice Teams gives security teams visibility into the highest and lowest risk people and teams so they know who to nudge (and keep an eye on). Aggregating information also makes it easier to gamify security to increase engagement and incentivize good security behaviors.

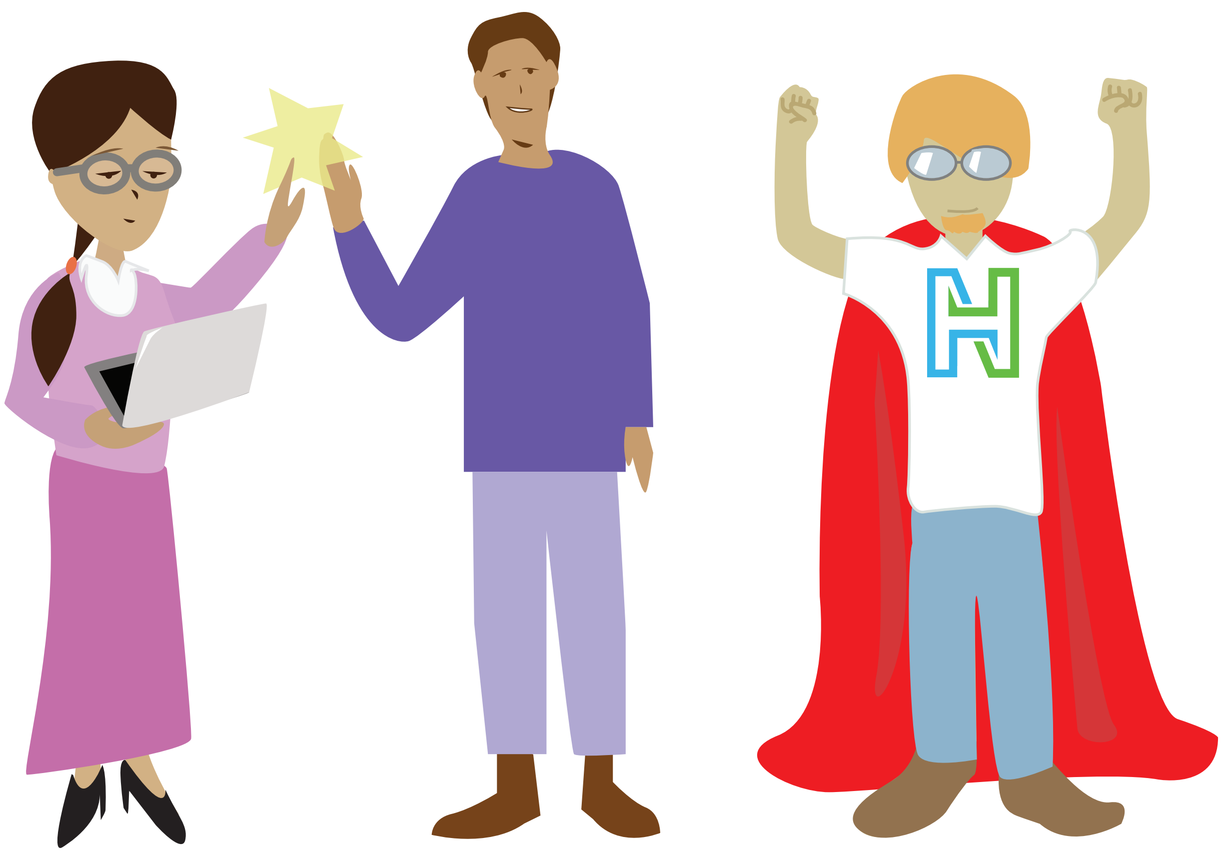
HackNotice Teams help you change the conversation within your organization, break down silos, and make cybersecurity a core objective rather than an afterthought.

Every single business process depends on technology, and our reliance on digital tools grows exponentially each year. But while tech's convenience and efficiency help us grow and achieve more, it also presents a host of risks. And although employees are becoming more fluent in digital processes, cybercriminals are also becoming savvier and more sophisticated.

Today, security is far too much for one person, one team, or one department to manage alone. Consistently defeating cyber threats requires a thorough understanding of security and unwavering commitment from every single member of your workforce.

However, a culture of security isn't something you can build overnight. It takes strategy, consistency, buy-in from senior management, and, most importantly, it takes visibility across your organization. By taking the appropriate steps and supporting your efforts with the right platform, you'll be well prepared to boost your security and drive your organization forward.

Interested in learning more about HackNotice Teams? Schedule a demo!



About HackNotice

HackNotice is a threat intelligence provider that helps consumers and businesses identify and protect against potential risks and respond to hacks through real-time alerts, around the clock monitoring, and actionable recovery recommendations. Indexing up to a quarter of a billion records each day, HackNotice provides users with the information and visibility they need to protect their digital identities. Founded in 2018, HackNotice is based in Austin, TX. For more information visit **www.hacknotice.com**.

3616 Far West Blvd #117 - 583 Austin, TX 78731 Phone: (833)HACK-900 eMail: contact@hacknotice.com