BITSIGHT®
The Standard in SECURITY RATINGS

The Secret to Creating a Cyber Risk-Aware Organization

BITSIGHT®

CONTENTS

BITSIGHT

INTRODUCTION

Who's responsible for a company's cybersecurity?

According to a 2018 survey from PwC, cyber threats are the number one concern of global CEOs — ranked higher than over-regulation, technological change, and even taxes. However, the job of protecting one's organization from cyber threats typically falls to security specialists in the IT department or is outsourced to a security provider.

How can ownership of the number one business concern belong to such a small group of people? The answer, of course, is that it doesn't. Talk to any IT security professional and they'll likely tell you that the responsibility for cybersecurity belongs to everyone, from the C-suite to contract workers to third-party business partners.

The process of mitigating cyber risk is not something that can be accomplished by technology or specialists alone. It requires of a culture of cyber risk awareness at your company in which every employee takes responsibility for cybersecurity.

Creating this culture, however, is easier said than done.

Talk to any IT security professional and they'll likely tell you that the responsibility for cybersecurity belongs to everyone, from the C-suite to contract workers to third-party business partners.

BITSIGHT

WHY CYBER RISK AWARENESS MATTERS

Do a Google Image Search for "cybersecurity," and you'll see one visual pop up again and again: a criminal in a black hood, hunched over a laptop, methodically hacking away at the mainframe.

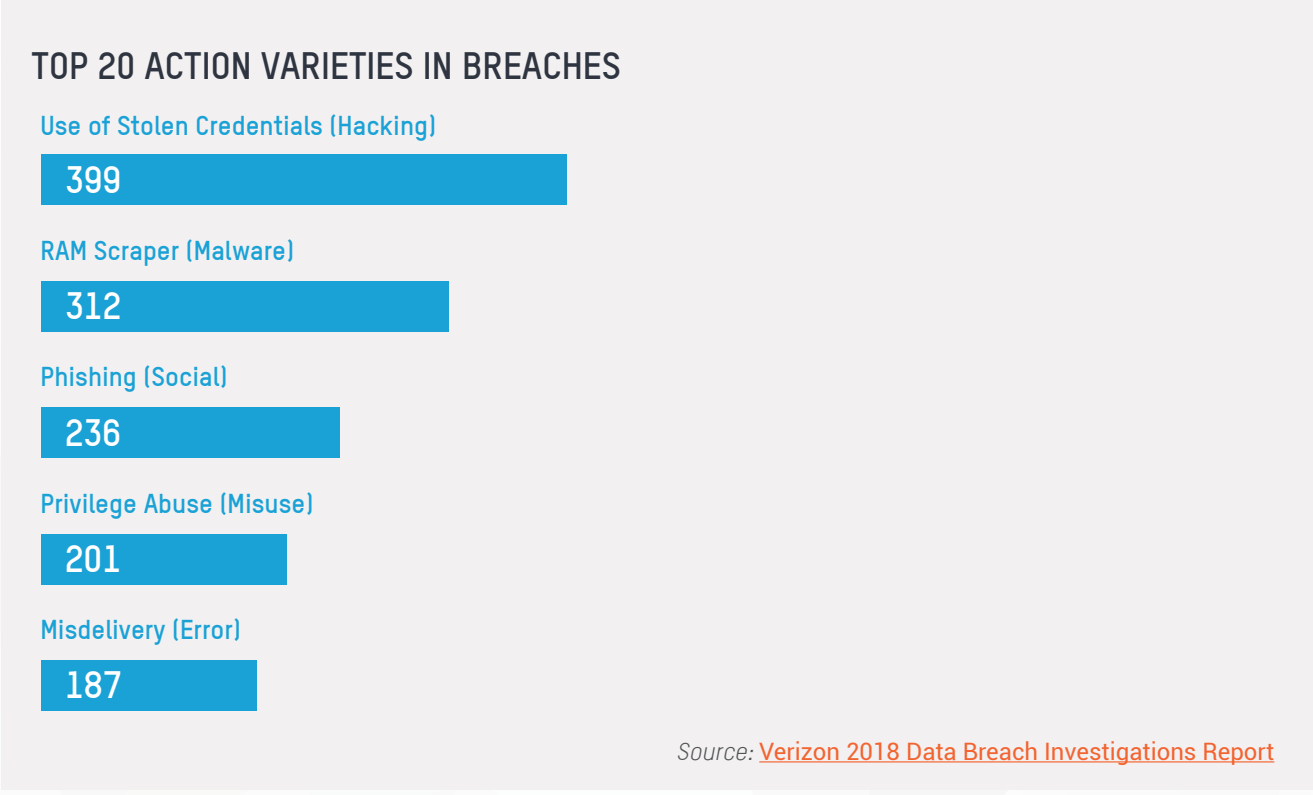
What might be more appropriate, however, is an image of your average employee, sitting at their desk, clicking a link in a suspicious email.

User awareness (or the lack thereof) contributes directly to a large portion of top data breach vectors

There are certainly bad actors out there attempting to infiltrate your organization's systems and steal your data. However, their method of attack is rarely a deliberate probe of little-known IT

subsystems. Instead, most hackers rely on manipulating unsuspecting employees to gain access.

User awareness (or the lack thereof) contributes directly to a large portion of top data breach vectors. According to Verizon, user-related risk vectors like phishing, privilege abuse, and misdelivery made up three of the top five action varieties in data breaches in 2017.



Source: Verizon 2018 Data Breach Investigations Report

Rather than force their way through a login screen, it's much easier for cyber criminals to take on the identity of an executive, an IT employee, or an accounts receivable rep and just ask for credentials. Alternatively, they can send users to fake login screens from which they can then harvest information. When employees are not aware of the latest phishing or pretexting techniques, or if they aren't making careful computer practices a priority, it is extremely easy to fall prey to attackers.

Email phishing is one of the oldest forms of cyber crime, and its continued use should be a clue to its effectiveness. According to the same Verizon report, email is by far the most common vector in social incidents and breaches, playing a role in 96% of reported attacks.

User error also contributes indirectly to many other cyber attacks. Malware and hacking with stolen credentials were the two most common action varieties in data breaches in 2017, and in many of those cases it's likely that the malware was installed or credentials were given out by misled employees who believed nothing was out of the ordinary.

When employees are not aware of the latest phishing or pretexting techniques, or if they aren't making careful computer practices a priority, it is extremely easy to fall prey to attackers.

WHY CURRENT AWARENESS PRACTICES DON'T WORK

Organizations are not blind to the importance of user awareness as part of corporate cyber risk mitigation strategies. In fact, security awareness training is a booming industry.

According to Cybersecurity Ventures, the security awareness training market is likely to grow from $1 billion in 2014 to $10 billion by 2027. As these numbers indicate, many organizations are hiring security training firms to help educate their employees and reduce their overall cyber risk. However, training alone isn't enough to create a culture of cyber risk awareness.

Not all training methods are created equal. When training is conducted in the form of a seminar, for example, employees might perceive the training as a kind of punishment. Lack of engagement from employees creates an environment where lessons are less likely to stick. In addition, research has shown that the effectiveness of anti-phishing training wears off over time.

PREDICTED GLOBAL SPENDING ON SECURITY AWARENESS TRAINING

2014

$1 BILLION

2027

$10 BILLION

Source: Cybersecurity Ventures

Knowledge without a feeling of responsibility does not necessarily reduce risk.

Other instruction methods like simulated phishing attempts and regularly scheduled computer-based training might be more effective, but still have some disadvantages. Security awareness training isn't cheap, and training activities take time that could be spent on revenue-driving work.

The central issue with security awareness training is that it focuses mostly on increasing the knowledge of employees. However, knowledge without a feeling of responsibility does not necessarily reduce risk.

When we ask employees to be more vigilant, we're asking them to do more work — work for which they're not being paid extra. In order to convince employees to change their behavior, we need to change their attitude, and that goes beyond education.

CREATING A FEELING OF RESPONSIBILITY

Why is it so hard to create a feeling of responsibility and accountability for IT security among an organization's employees?

The issue is that success in cyber risk mitigation is measured by a lack of negative results. In other words, the best workday for a cyber risk professional is a day when nothing happens. The feelings of success and gratification that accompany many business activities — making the sale, finishing the project, beating the projections — are absent in the world of cybersecurity.

There is also the matter of cybersecurity being a highly technical subject. Your average non-IT employee is used to deferring to the IT department for their technical needs, and therefore might not be inclined to gain an understanding of complex IT processes. This lack of cross-departmental knowledge might lead some employees to have more faith than is warranted in the ability of cybersecurity personnel to stop attacks.

In an ideal world, the threat of a massively damaging data breach or cyber attack would be enough to motivate employees to take responsibility for cyber risk awareness. However, you could also say that the threat of a car accident should be enough to motivate people to drive safely. It's not, which is why we have police officers on the road to enforce speed limits and stop signs.

So, organizations are left with two choices: wait for the major cyber attack that motivates employees to take responsibility for adopting cybersecurity best practices, or introduce accountability in order to create an organization-wide culture of cyber risk awareness.

The feelings of success and gratification that accompany many business activities — making the sale, finishing the project, beating the projections — are absent in the world of cybersecurity.

People are already aware of the danger of not paying close attention to their emails or clicking on suspicious links. Hearing once again that they could cause the next mega-breach has not been enough to motivate them so far.

THE VALUE OF EVIDENCE-BASED AWARENESS

In order to begin taking responsibility for their actions or non-actions, employees need to be able to see the results of those actions or non-actions. There needs to be some level of visibility into the effects of security awareness training, otherwise employees won't be able to see the benefits of following the guidelines put forth in that training.

The challenge is that cyber risk has historically been difficult to quantify. The metrics that are readily available to measure cybersecurity are typically very technical, and therefore not beneficial for motivating employees outside of the IT department. As a result, attempts to motivate workforces into improving their risky online behaviors have typically relied on hyperbole, scare tactics, or other exaggerated messaging.

A 2017 paper in Government Information Quarterly puts it this way: "Cybersecurity specialists often attempt to use message framing, but often fail to get the right message across. They use management guru techniques and manipulate common cognitive vulnerabilities in order to over-dramatize and over-simplify cybersecurity risks...This does not result in the attention desired: critical systems remain unprotected and behaviour does not change or cybersecurity protection is delegated to software and hardware providers."

In other words, people are already aware of the danger of not paying close attention to their emails or clicking on suspicious links. Hearing once again that they could cause the next mega-breach has not been enough to motivate them so far.

As a result, organizations rely more and more on technology-driven cybersecurity solutions, creating a false feeling of security among employees, who likely believe that someone downstream will take care of any employee-caused security events.

The way out of this vicious cycle is evidence-based messaging. As the authors of the Government Information Quarterly paper write, "Simple message frames do not work for cybersecurity and therefore evidence-based message framing is necessary."

BITSIGHT

MEASURING AWARENESS

We've shown that training alone is insufficient to create an organization-wide feeling of responsibility for cybersecurity, and identified that the missing pieces are visibility and accountability. But, as we've mentioned, visibility into cybersecurity performance is hard to come by.

The key to effective cyber risk awareness is visibility and accountability. That means finding evidence of awareness that is quantifiable, easy to understand, and consistently updated.

EFFECTIVE EVIDENCE FOR CYBERSECURITY AWARENESS IS:

Quantifiable

Easy to understand

Consistently updated

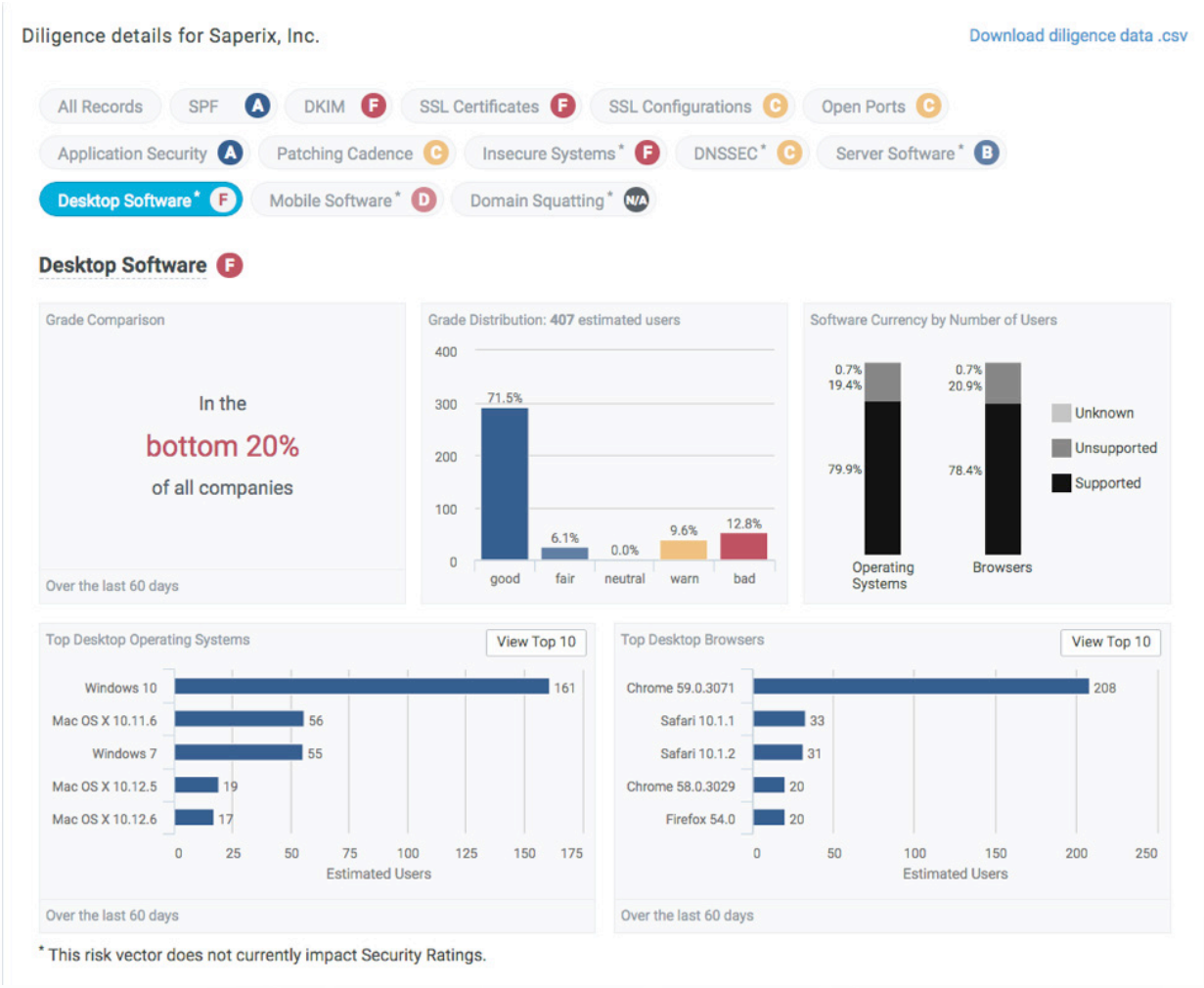
Security ratings are a tailor-made solution to this problem. Security ratings are automated assessments of an organization's cybersecurity performance based on externally observable risk factors.

On platforms like BitSight, these ratings are delivered in two forms: an overall rating that indicates the security posture of the whole company, and individual ratings for certain risk factors like botnet infections, TLS/SSL certificates, and open ports.

By identifying which risk vectors directly or indirectly relate to user behavior, CISOs and other security professionals can use quantitative metrics to inform cyber risk awareness performance. On the BitSight platform, vectors which could be used include:

- File Sharing
- Disclosed Credentials
- Malware Servers
- Botnet Infections
- Patching Cadence
- Public Disclosures

Each of these risk vectors comes with a grade of A-F for performance compared to best practices.



BENCHMARKING CYBER RISK AWARENESS

Security ratings can be used to create quantitative measurements of cyber risk awareness. All that's left to do is put these measurements in context in order to motivate employees to maintain vigilance when interacting with technology.

Benchmarking is the best way to add context to these measurements. By benchmarking risk vector ratings that reflect security awareness and comparing results to historical numbers, other business units, and competitors, security professionals can finally add evidence to their organization-wide cybersecurity messaging and effectively reduce the risk of cyber attack.

Benchmarking Historical Security Performance

Security ratings allow users to view historical performance in specific risk vectors. BitSight, for example, shows historical data going back twelve months. When a security professional logs into the BitSight platform, they can create reports comparing grades in, say, file sharing performance against the same category in previous months.

There are a few uses for this strategy. First, CISOs can finally make objective assessments of the effectiveness of their security awareness training efforts without having to pay consultants for expensive and time-consuming testing. By simply comparing performance in specific vectors from before and after a training initiative, one can see whether or not it worked.

Going deeper, security leaders can use trends in performance to plan an optimal security awareness training schedule. Since it's been proven that the effectiveness of security awareness training wears off over time, frequent training is required to truly create a cyber risk-aware organization. By setting a benchmark for an acceptable grade in each risk vector, then tracking how long it takes to fall below that threshold, the proper frequency for training becomes clear. This saves security leaders from spending too much or too little on security awareness training.

Benchmarking Across Business Units

Another way security leaders can motivate employees to take responsibility for organizational cybersecurity is by fostering a sense of healthy competition between business units and subsidiaries.

By dividing an organization into segments (i.e. specific branch offices, regions, or subsidiaries), then comparing awareness performance across these segments, security leaders can appeal to the competitive side of their employees. Just as one might compare sales numbers between the New York and LA offices to motivate a team, with BitSight, CISOs can compare ratings in awareness-related risk vectors.

This kind of insight can also help cybersecurity decision makers focus their security awareness training efforts on the parts of the organization that need it most. A hyper-targeted investment in awareness training for the lowest-performing business units can improve the posture of the entire company.

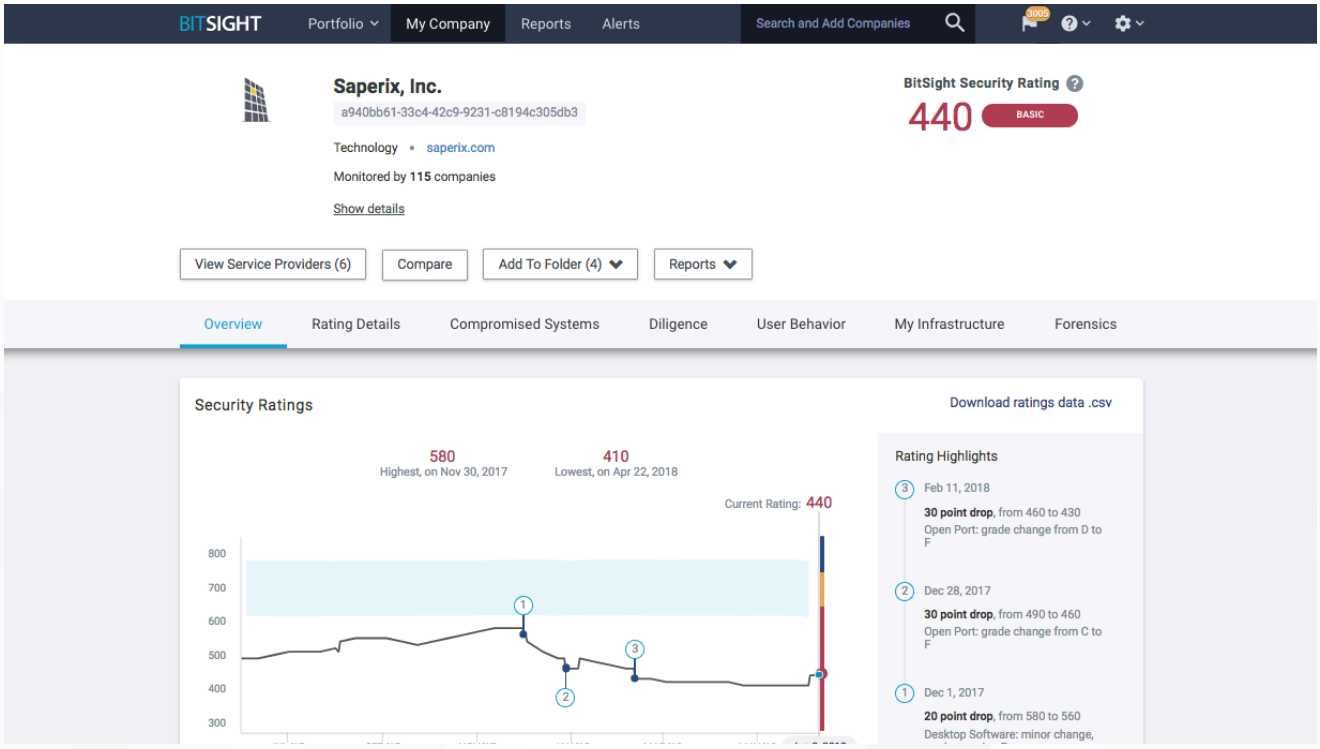
Benchmarking Using Competitors or Industry Average

Because security ratings are based on externally observable information, they can be accessed by users outside of the organization in question. So, while simulated spear phishing results from your competitors might be a well-guarded secret, their security ratings in awareness-related risk vectors are not.

A hyper-targeted investment in awareness training for the lowest-performing business units can improve the posture of the entire company.

This gives security leaders unprecedented insight into how their awareness efforts compare to their competitors. BitSight even organizes data into groups of businesses to represent an industry average — giving users an excellent benchmark to use for goal-setting and strategic planning.

Having this industry-wide information allows security leaders to have data-driven conversations with the Board and members of the C-suite regarding cybersecurity awareness. When asking for increased resources for awareness training, for example, it's extraordinarily useful to be able to point to a competitor and show that their awareness performance is outpacing one's own.



BITSIGHT

CONCLUSION

Social attacks like phishing and pretexting cost organizations massive amounts of money, damage reputations, and lead to regulatory consequences. They continue to be a popular method of cyber attack, and cause hundreds of data breaches each year.

In order to combat these attacks, many organizations invest in security awareness training. However, without a shared feeling of responsibility for cyber risk mitigation throughout your organization, this training is likely to fall on deaf ears.

The secret to creating a cyber risk-aware organization is to add evidence-based messaging to one's security awareness efforts. Tools like BitSight Security Ratings are the best solution for benchmarking performance in security awareness and adding context to conversations about cybersecurity.

Equipped with an understanding of the results of their actions, employees will begin to take responsibility for how their interactions with technology could affect the organization as a whole. When everyone works together to protect the well-being of the company, everyone benefits.

What's next? It comes back to a simple framework: visualize, prioritize, act. Security ratings can be used to look past awareness and visualize the effectiveness of other cybersecurity controls. Then, security leaders can use benchmarking to identify and prioritize areas of cyber risk which could have the greatest impact on the organization. Finally, they can take action, resolve issues, and mitigate risks.