BEAUCERON
SECURITY

THE DEFINITIVE GUIDE TO SUCCESSFULLY IMPLEMENTING SECURITY AWARENESS

HOW TO HELP YOUR TEAM CARE MORE ABOUT SECURITY.

Security awareness is not only an IT issue

Security awareness is an organization-wide concern that affects every person in a business, non-profit, charity or government.

It's about creating and sustaining positive individual behaviours and an organizational security culture. It's not just about computer-based training and phishing, though these are important activities.

Whether this is your first security awareness effort or campaign, or you've been leading the charge for years, there's always room for continuous improvement.

TABLE OF CONTENTS

INTRODUCTION

Look out for this icon! We've added our own aggregate data from a sample of more than 23,000 users.

The people in an organization are its greatest strength.

It's easy to fall into the trap of blaming users for falling victim to phishes, for breaking a policy and storing information in personal cloud sites, or any other number of errors, mishaps or mistakes.

But people are not the problem; they are the most valuable resource for any organization and a crucial part of a well-rounded cybersecurity plan.

By empowering your people to understand cyber risks and how their decisions can have a massive positive–or negative– impact on your organization, you'll create a culture of security that will complement the technological security controls you've put in place.

Security awareness can't replace the need for core security tools, but these tools can't replace the need for awareness programs either.

Creating and sustaining a security culture takes a combination of planning, key communications, change management, technology and buy-in from the most senior leadership to the front-line of any organization. A culture of security goes beyond simply making people aware of security – it's about helping them care about security enough to take simple steps to dramatically reduce risk.

> *Security awareness enhances their ability to recognize danger and desire to protect themselves and their organization*

WHAT IS SECURITY AWARENESS?

In our research, 92% of employees think they play an important role in protecting their organization against cyber threats. However, a third of them believe they don't receive enough training to make a difference.

Security, at an individual level, is the attitude and knowledge someone holds about risks to physical and informational assets and how to mitigate those risks.

Security awareness training educates and trains employees, so they understand the importance of, the risks to, and their role in protecting information and assets. Awareness training isn't an end in and of itself, but a continuous feedback loop between individuals and the organization on identifying and discouraging risky cyber behaviours, and recognizing and promoting good cyber behaviours.

As the U.S. National Institute for Standards and Technology (NIST) points out, "security awareness efforts are designed to change behavior or reinforce good security practices." In other words, security awareness training is the first step towards changing individual behaviours and building a culture of security in an organization by empowering people.

> *Security awareness is a continuous effort that aims to instill a security culture; empowering people to be in control of technology.*
>
> *— The Beauceron Pack*

WHY DOES SECURITY AWARENESS MATTER?

94%

of malware detected in median companies was received via email.

(Verizon, 2019)

1/3

of workers rarely or never think about cybersecurity at work.

(Tessian, 2020)

96%

of IT workers said security training was at least somewhat effective reducing incidents.

(CIRA, 2019)

Phishing

remains the single largest tactic used by criminals in data breaches.

(Verizon, 2020)

What do these numbers tell us? Humans are the primary target of cybercriminals. Security awareness matters because it unleashes people's potential to reduce risk to physical and informational assets.

People can't protect against risks they don't see or understand. Security awareness enhances their ability to recognize danger and desire to protect themselves and their organization.

Do you want to learn more? Check out these infographics on cyber crime and phishing trends.

If you want more resources to share with colleagues, download these free infographics on how to protect yourself, and how cyber threats work and affect you!

DOWNLOAD

WHAT ARE THE FIVE STAGES OF A SECURITY AWARENESS PROGRAM?

YOUR PLAN

The first step in building a security awareness program that **empowers people and reduces cyber risk** is determining the status quo. Do you already understand your organization’s threats, policies, regulatory requirements and business goals? Are you doing any security awareness activities already? If you are, are those activities aligned with your risks, policies, regulatory requirements and goals?

Once you’ve analyzed your current status, you need to find out what resources you have available to implement or enhance your security awareness program. What have you been tasked to do? How much freedom do you have? What is the existing budget for security awareness?

DEVELOP A BASELINE

Surveying your community before starting any awareness effort is a best practice supported by experts and researchers. But developing a survey, picking the questions and answers, and reviewing the results is far easier said than done for most organizations (even those with dedicated security awareness teams).

> ***Our recommendation:*** *Don't re-invent the wheel. Use established templates or, better yet, pre-built surveys if they're available in the technology tool you select to help you build, launch and measure your awareness efforts. Bonus: using a standardized survey will allow you to compare your organization's responses pre- and post-campaign with others'!*
>
> *By giving a voice to your community and responding to their feedback in a timely fashion, you'll build greater engagement, buy-in and some critical metrics all at the same time!*

EDUCATE AND TRAIN

After you've surveyed your users, it's time to educate them on key risks in accordance with best practices, your organization's goals and their individual needs. Plan your content based on the biggest gaps revealed by your surveys and make it **relevant to your team**.

A key goal of your awareness content is to educate your team that cybersecurity is not exclusively an IT issue, but a business issue that concerns everyone in the organization. Also, be sure to test users on their understanding of the content. Some things you may think are simple don't necessarily come easily to everyone. If your team isn't learning from the content you're providing, you know it's time to develop or acquire new content.

SHAPE BEHAVIOURS

The first step in shaping behaviours is measuring for the presence or absence of positive or negative security behaviours.

Effective measurement of security awareness requires more than quizzes at the end of training sessions or online learning modules (though those are an important component!). Once you've made your community more aware, it's critical to give them a chance to put that knowledge to use in a safe, constructive and realistic way.

That's where tactics like **phishing simulations** come in. Including phishing simulations in your program gives your employees the opportunity to demonstrate

95% of respondents said they were aware that their organization has policies on information security. However, specific areas such as policies on personal device usage or how to safely work remotely were not widely understood.

positive security behaviours such as spotting and reporting phishing. When people fall victim to a phish, there is an opportunity to provide additional training so they learn how to detect future phishes.

You can also use phishing simulations to reinforce positive security activities. Leading edge phishing simulation programs don't just reward people for not falling victim to a phish; they also give rewards for reporting a phish even if they first fell victim to the simulation. They're rewarded because reporting the phish demonstrates that they know how to get help in the event of a real phishing attack. This model reinforces that making a mistake is human and the most important action a person can take even after making a mistake is to report it and ask for help.

Click here for some free infographics to teach employees **how to spot a phish** .

REINFORCE WITH FEEDBACK LOOPS

Security awareness and behaviour change is never a one-and-done effort. Your program will only work if it is continuous. Training employees once during their onboarding will not instill a cybersecurity culture. Security risks, criminal tactics, organizational policies and tools all continuously change and evolve. **Your training and testing must keep up with those changes.**

A continuous training program doesn't just keep everyone up to date, it's also a signal from the organization's leadership that security is a priority and a key part of all jobs.

> ***Our recommendation:*** *Survey your employees at least annually and at most bi-annually. Conduct core training during employee onboarding. Supplement onboarding training at least every year with updated educational materials that give examples of current and expected cyber threats and risks. Ideally, schedule additional topical content quarterly. Leading programs also provide users with educational libraries they can access on a voluntary basis.*

WHY DO MANY SECURITY AWARENESS PROGRAMS FAIL?

Security awareness programs often fail in organizations of all kinds and of all sizes for the following reasons:

1. They are viewed as IT-department driven activities that are about telling people 'no.' They don't focus on or celebrate positive security knowledge or behaviour.

2. They are often overly focused on phishing as the major metric of success. While phishing is an important tactic, it's a fraction of what security awareness and behaviour change is all about.

3. They don't make the content contextual and specific to an organization.

4. The success metrics are mainly based on execution rather than effectiveness. Attendance at an in-person event or roadshow, and completion rates on computer-based training doesn't mean that awareness training has been done well, successfully or with meaningful return on investment.

5. A common mistake in the phishing simulation component of many security awareness programs is punishing people for falling victim to a simulation (or after a certain number of simulations). Some organizations even use phishing simulation results as a cause for ending someone's employment. We don't recommend or encourage that approach. The reality is, on the right day with the right targeted phish, anyone can fall victim to a phishing simulation.

DESIGNING A SUCCESSFUL SECURITY AWARENESS PROGRAM

A security awareness program that takes a positive view of the potential of people to be part of the solution – rather than the problem - will result in higher engagement, greater security culture buy-in and significantly reduced risk.

LEADERSHIP SUPPORT

If your board of directors and senior leadership team care about security, you stand a far better chance of influencing other leaders and their teams to develop a security culture.

If leaders don't care about security awareness, it may be because they don't realize how important it is: dollar-for-dollar, it's among the most cost effective and quickest ways any organization can reduce risk.

New security awareness compliance requirements imposed by government regulations or legal agreements often garner executive and board attention. What gets you budget and buy-in, however, is demonstrating that a well-executed security awareness program tangibly reduces cyber risk and provides excellent return on investment (ROI). To help relay the urgency and significance of security projects, spend time clearly articulating how the security strategy will help the organization achieve its overall strategic plans.

> *A continuous training program doesn't just keep everyone up to date, it's also a signal from the organization's leadership that security is a priority and a key part of all jobs.*

HOW TO GET THE SUPPORT YOU NEED:

A) STATE THE VALUE YOUR PLAN WILL BRING

As the security professional, your job is to paint the picture of how security fits into the organization's strategic objectives. The leadership team and your board will want to know the impact that your security plan will have on the business. Make sure to state the value that investments will bring to the organization. For example, a cybersecurity strategy could avoid unscheduled downtime in the case of a ransomware attack.

B) TRY TO USE THE LANGUAGE THAT YOUR LEADERSHIP TEAM IS FAMILIAR WITH:

For you, terms like BYOD, SIEM, cloud computing, DDoS, etc. are your everyday language. Consider that they might not be familiar with technical terms, security tools and technologies. Using less jargon will enable better communication.

Try talking about: reputation impact, financial impact, board governance and responsibility and business impact.

C) LEAN ON REAL-LIFE EXAMPLES

If you just showcase the problem, you won't have the impact you want. Bring recent news articles that show the consequences of not implementing proper cybersecurity measures. Use case studies highlighting positive changes other companies saw when they implemented a security culture.

> *Get relevant numbers like a measurable progression in your cybersecurity maturity level, the percentage of risk that could be reduced using your strategy, the budget you will need to implement the strategy, what would be the return on investment, and more.*

D) TALK ABOUT RATIONALE IN SELECTING YOUR PRIORITIES

Describing the current vulnerabilities, risks and immaturities will be beneficial if your plan then tackles them to turn them into strengths. Your current position does not have to be a negative one. You can explain it as things that could be improved and how those improvements will benefit the company.

> *Consider what needs to be done immediately and what can be planned for the future.*

E) HOW IS IT GOING TO WORK?

Your plan sure looks awesome, but you need to have the logistics in place. Determine the measures of success and explain them. Let them know how you are going to report on your projects and if you will need help from other departments.

LEVERAGE THE RIGHT METRICS

A successful security awareness program demonstrates how security behaviours have changed. In order to show the ROI your leadership is looking for, you must evaluate perceptions and practices both before and after awareness campaigns to see if you've made progress.

One evaluation method we've discussed is surveys; they can be a highly cost effective and efficient way to gather actionable insights regarding users' perceptions of cybersecurity. Find out: how many people view cybersecurity as a risk to their organization? How many people view their organization as a target for cybercrime? How many people think their leadership team values cybersecurity?

One of the most popular metrics is phishing simulation campaign results. In the past, click rate has been the industry standard for success, but it can be misleading if only viewed in isolation. Click rates can be highly subjective – was the phish easy to spot or hard, was it tailored to the organization or generic?

In order to measure change in behaviour consider more nuanced metrics offered by next generation security awareness platforms. What are some more nuanced metrics, and how are they useful?

A. The ratio of people who fell victim to a simulated phish to those who didn't and reported doesn't just measure susceptibility to phishes; it measures how many people spotted the phish and reported it, which is the most important behaviour to create and consistently reinforce.

B. Time-to-report and time-to-fall-victim statistics will provide your organization with baselines that can be useful when reviewing how fast your incident response team needs to move on new real attacks.

C. Emotional tagging of phishing simulations gives you insight into why people fall victim to a particular phish by identifying which emotion was successfully targeted in the phishing simulation. This allows you to customize education based not only on the technical signs of a phish, but the emotional levers as well.

> *Consider combining various standalone metrics (click rates, report rates, education scores, whether people show up in known data breaches) into an overall security score. This provides a more complete and balanced view than a single metric on its own.*

FOUR TIPS TO START BUILDING A METRICS-DRIVEN CULTURE TODAY

1. Start by creating a baseline survey to learn where your employees are in their cybersecurity journey. Make it anonymous so that they feel comfortable telling the truth. Include the questions that concern you regarding the awareness of your company's processes.

2. Review your current cybersecurity policies and update them with your team. Take the time to explain the role that each employee plays. You can download free policy samples **here**.

3. For those who already have a campaign in place, think about testing your employees at the end of their learning sessions/campaigns. This can highlight the areas where your team is excelling and give you an opportunity to recognize that positive behaviour publicly. Too often we focus on the weaknesses, but it is far more powerful to reward the employees who are taking the right steps.

4. For teams with well-established security metrics, take your process a step further by conducting an analysis of of your results. You may have your numbers for each campaign, but your need to know what they mean together.

SELECT THE RIGHT TECHNOLOGY TO POWER YOUR PROGRAM

Our survey told us that 31% of employees see cybersecurity as an IT issue instead of a business issue. We must explain how adopting a security culture is beneficial to everyone even in our personal lives.

Trying to run a security awareness program without the right technology results in hundreds of lost hours of productivity. It makes it far harder to scale a program and to focus on continuous improvement. The right platform can save up to three full-time positions in person hours, giving even the smallest of teams the capabilities of a Fortune 500 firm.

Select a partner who is as passionate about your organization's security awareness goals as you are. They must provide tools that can optimize your efforts and maximize your program's impact; look for compelling content and an engaging experience that will help your community care about their personal security. Find a tool that makes it easy for you to survey, train, test and then review your progress so you can continuously evolve your program.

> ***Our recommendation:*** *Look for a tool that has a course editor built in so that you can customize courses based on your policies and culture; learn more about why this is important in the next section.*

ADAPT THE CONTENT TO YOUR OWN CULTURE

Generic, off-the-shelf content can be useful as a part of your program but shouldn't be the only material you serve to your community. Use great content to educate on cybercriminal techniques like phishing, and to explain to your audience why they are a target as an individual and why your organization is a target.

With the right content creation and distribution tools, you can create powerful content to tell your organization's security stories in ways that make security relevant and drive organizational members to care about preventing or responding to attacks.

> ***Our recommendation:*** *create content that talks about the most common attacks your team has seen. Give examples from your industry, geographic region or news stories.*

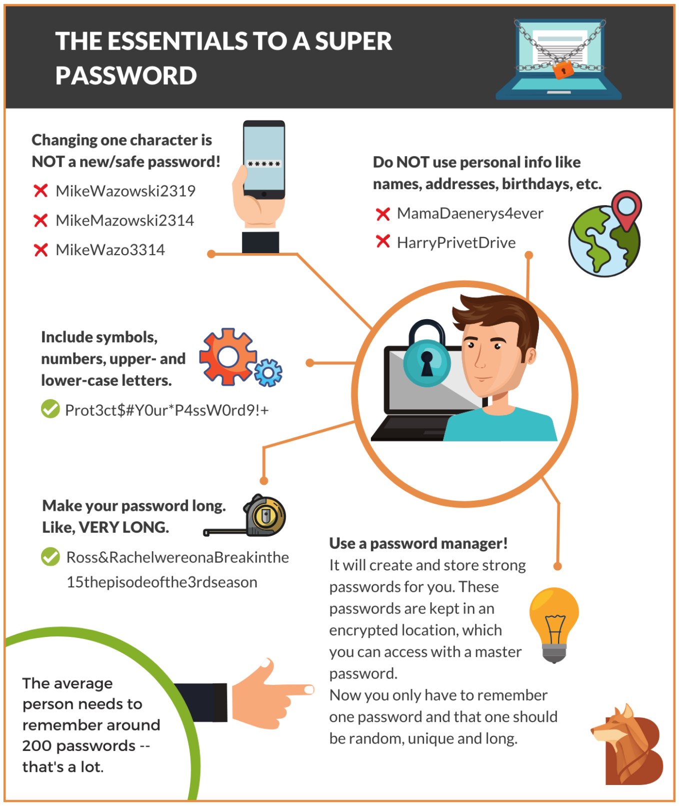
> *Providing contextual and relevant content is the most important part of your awareness campaign. The more you can customize content to reflect your organization's risks, policies, procedures, and approaches, the more your users will find it useful and engaging.*

TEACH THE WHY AND THE HOW

Most awareness programs —of any kind— focus on the 'don'ts: "don't do X". What they are not doing is explain why.

Go beyond the 'don'ts' and explain why actions such as re-using passwords is so risky online. Provide clear examples of how your team can reduce this risk using approaches such as multi-factor authentication or other tools your organization provides or supports.

Help your community understand what your policies are on information security, acceptable use, secure remote work and more by providing education that explains the why of the policies and how your organizational members can adhere to the rules of the digital road. People respond better to information when they understand why and how it's important. Policies, training and educational material should all express the impact they will have if completed appropriately.



THE ESSENTIALS TO A SUPER PASSWORD

Changing one character is NOT a new/safe password!

- ✗ MikeWazowski2319
- ✗ MikeMazowski2314
- ✗ MikeWazo3314

Do NOT use personal info like names, addresses, birthdays, etc.

- ✗ MamaDaenerys4ever
- ✗ HarryPrivetDrive

Include symbols, numbers, upper- and lower-case letters.

- ✓ Prot3ct$#Y0ur*P4ssW0rd9!+

Make your password long. Like, VERY LONG.

- ✓ Ross&RachelwereonaBreakinthe15thepisodeofthe3rdseason

Use a password manager! It will create and store strong passwords for you. These passwords are kept in an encrypted location, which you can access with a master password.
Now you only have to remember one password and that one should be random, unique and long.

The average person needs to remember around 200 passwords -- that's a lot.

PARTNER WITH KEY DEPARTMENTS

Changing cybersecurity behaviours across the organization requires buy-in from each department. Get buy-in by engaging department leads in the planning of your program and incorporating specific risks relevant to their team in the training mix. If department leads know you care about their goals and their team, they're more likely to participate and even become an active champion of your program.

Take into account that some departments may be more exposed than others; they might receive different threats and require specific training.

Seek out allies. Your legal or risk teams could help you with compliance. Marketing can help review or even create new material for your campaign that creates connection between your organization's reputation or brand and security. Many human resource departments are great allies in security programs; in turn, your program will support their efforts to help nurture the potential of the people in the organization.

> *Make it easier for department leads to see their teams' progress with a dashboard that gives them insight and a sense of program ownership. This helps reinforce security as an organization-wide value, not just the IT department's problem.*

CREATE EFFECTIVE PHISHES

The goal of any phishing program is to prepare and educate individuals on how to spot and report a phish. It's not about tricking people- it's about creating effective learning experiences. Security professionals need to have the skills to think like an attacker and be able to mimic attacks their organization is receiving.

LEVERAGING THE DATA TO REDUCE RISK

While the pure click rate of phishing simulations is an important metric for an organization to track, it's arguably more important to track the time to click, the time to report and the reporting rate of phishing simulations.

Tracking, the amount of time it takes for users to click a phishing simulation, and the time is takes for users on average to report, can drive discussions around incident response. For example, if you realize 25% of users that fall victim do so outside of regular business hours, it may be time to investigate the organization's after-hours incident response.

HOW DO I BEST SIMULATE REAL ATTACKS?

The reality is that most attackers do not send all employees the same phish, at the exact same time, on the same day. Therefore, you should try and resemble read practices as much as you can! This is where the security professionals put their "hacker hat" on and think of how they would try to gain access to the organization.

As with everything in security awareness, how to simulate the attacks depend on the organization. We recommend for organizations to evaluate their risk tolerance.

CAMPAIGNS OR RANDOM PHISHING?

For organizations with a high-risk tolerance, the most effective way to simulate attacks is run fully automated, randomized phishing simulations. That is, setting up your approved bank of phishing templates then letting the platform randomly select times for the phishing simulations to be sent.

For organizations with a lower-risk tolerance, leverage the random, automated phishing simulations to ensure a solid baseline of attacks. Take it the next level by incorporating highly targeted campaigns or spear phishing to focus in on different individuals or departments.

BE WARY OF THE "GOPHER EFFECT"

We have found that scheduling one large campaign, running at a specific time with a specific template can often create a "gopher effect", where employees will start notifying each other of the phish. These campaigns often take several hours to land in your users' mailbox, and by the end of the day your results start to become skewed by having employees passing the message around. While it is great news that employees are warning others of suspicious e-mails, it can heavily skew your results.

HOW DO I AUTOMATE MY SECURITY AWARENESS PROGRAM?

In our survey of 23,000+ people, more than 800 users said they had shared their passwords because it was necessary for work purposes. Make it easy to make the right choice: consider whether updating your processes and/or technologies can end such a risky practice.

Leverage your security awareness platform to automate as much of your program as possible, freeing you up to focus on where you can make the most impact: planning, content and reviewing metrics.

AUTOMATE AND RANDOMIZE PHISHING

Fully automating your phishing campaigns saves hundreds of hours of your time every year. Randomizing your campaigns using a 'phish tank' of various phishes that are distributed amongst your team at random times will also result in more relevant metrics that reflect the diversity of real phishes and real attacks that are active against your organization 24/7.

With your newly freed time, you can focus on targeted spear phishing campaigns to take your program and people to the next level.

BEHAVIOUR INTERVENTION

After a user has fallen victim to a simulated phish, don't make the mistake of relying on the landing page content as the only source of remedial education: 90% of users panic after clicking a phishing simulation and close the landing page within seconds of realizing they made a mistake.

Instead, leverage a platform that can assign **follow-up training to the user automatically**. But what if team members ignore this material? After all, what's in it for them?

Create a positive incentive for taking remedial training. Reward team members who fall victim but who take remedial training and report their phishing simulation even after falling victim. This reinforces their learning and allows them to demonstrate behaviour change.

HOW DO I DEMONSTRATE THE EFFECTIVENESS OF MY PROGRAM?

CYBER RISK

THE REDUCTION IN CYBER RISK

Showing that your program has helped your company keep their data, assets, and staff safe is the best way to obtain more resources and support later on. Keep up reporting and tracking metrics!

Show the difference between the data gathered prior and after running your campaigns. Illustrating the improvement and articulating how the program will continue to help the organization improve can support additional security projects, such as two-factor-authentication.

CYBER CULTURE

THE EVOLUTION OF YOUR SECURITY CULTURE

The ultimate goal of your security awareness program is behaviour change. By dividing the awareness evolution of your community into defined stages you can better track and measure the progress of your security program.

Stage 1 ▶ Individuals understand why cybersecurity is important to them, and their role. Measure through training, completion and surveys.

Stage 2 ▶ Transition awareness into knowledge. Individuals know what to do, and are able to act on it. Behaviour starts to change. Measure through metrics such as phishing reporting rates.

Stage 3 ▶ Knowledge evolves into 'Security-By-Design.' This is when behaviour becomes part of roles, processes and procedures within an organisation and is reflective of a robust security culture.

When people are motivated to seek out knowledge beyond that required by their jobs, you've identified champions and allies. This activity can be measured by voluntary consumption of education.

COMPLIANCE

REGULATORY COMPLIANCE

Demonstrate adherence to all the compliance regulations your company must follow.

Depending on where your organization does business, you will either have to comply with PIPEDA (Canada), LGPD (Brazil), CCPA (California), HIPAA (U.S. medical data), or GDPR (Europe).

Being compliant will reduce your cyber risk, minimize fines if you are ever breached, ensure you have a response plan and build trust with your customers. If you're in a heavily regulated industry, you'll need to make sure you can run reports in real-time so that you can quickly demonstrate compliance without needing to move data into a CSV.

ROI

RETURN ON INVESTMENT

The best way to demonstrate return on investment to senior leadership and the board is by talking about time savings in terms of dollars and cents.

For example, you have 1000 people and every year 200 people were falling victim to a phish (20%). After a year of security awareness, you are able to reduce the phishing click rate from 20% to 5%. Now, the organization has gone from falling victim to 200 real phishing e-mails to 50. Consider how many hours were saved by not having to clean up the extra 150 incidents. With the reduction in real clicks, there's also a significantly lower likelihood that the right phish hitting the right person could result in a full-out data breach or financial fraud costing hundreds of thousands or millions of dollars in cost.

> *Investing in security sends a strong message to customers and prospective investors that you are worthy of their trust; putting security at the forefront can differentiate you from your competitors.*

In our research, 92% of employees think they play an important role in protecting their organization against cyber threats. However, a third of them believe they don't receive enough training to make a difference.

Follow our blog for informative articles on cybersecurity at:

WWW.BEAUCERONSECURITY.COM/BLOG

Want to learn more? Book a demo!

WWW.BEAUCERONSECURITY.COM/DEMO

Chat with us: (877) 516-9245