TQ Security

by Accenture

Resume Course

Bookmark Add to Channel Download Course Schedule Reminder

Table of contents Description **Transcript** Exercise files Discussion Related C

TQ Security Preshow

Transcript links

TQ Security Preshow

Hi, everybody, Kelly Bissell here. Welcome to Security TQ. As the global lead for our security practice, I'm inspired every day by our people . We work tirelessly to keep our clients secure. From innovative solutions to the best teams in the business, I think we serve our clients better than anyone. But I know security can feel a little bit intimidating when you don't really work in it every day. So we're going to do our best to make security seem a little more approachable and get you more familiar with our people and our capabilities. When big security breaches happen, it always makes the news. And I know many people are really familiar with Edward Snowden leaking classified U.S. Government information, or the Yahoo data breach, or Target, or others that you've seen in the papers. But let's take a second to think about what doesn't make the news. The millions of unsuccessful attempts that are blocked on a daily basis. Companies are protected against those hacks because they have strong security programs in place. The threat landscape is growing quickly, hackers are getting smarter, and there's not a single industry or a company that doesn't need to prioritize security. So we need to continue to innovate and deliver solutions that keep our clients steps ahead of the hackers. We don't want them just to be protected against known threats. We want their systems and platforms to be secure against threats that may not even exist yet. Our mission is that Accenture is going to secure the world, which means that everything we do is done securely. If we migrate a client's environment to the cloud, it's a secure migration. If we're delivering a new application, it's a secure app. If our clients are deploying a new banking system, we're going to make sure that it's secure for their customers. Or if our clients have manufacturing or energy plants, we secure them for consistent electricity and gas delivery to the world. We want Accenture's projects to be secure from the start, which requires security to be a constant design item, not an afterthought. Our security solutions are tailored to industries and clients in which we serve, adhering to specific regulations and compliance standards. But the core principles of security are constant, keeping the world's data safe and private. At Accenture, we've been delivering secure solutions for clients for over two decades. That's right. We've been building our security expertise for 20 years, for the benefit of keeping our firm and our clients safe. And I don't mean to brag, but we have some pretty impressive credentials to back us up. Just to name a few, we have over 800 pending and issued patents that involve security problems. We built 7 Cyber Fusion Centers where we host interactive workshops and demonstrations of our latest innovations and capabilities to help our clients know their threats, test against those threats, and expel those threats. We leverage 2 Cyber Labs where we can develop research driven solutions to help our clients see future threats, what to expect the landscape to look like 3 to 5 years from now, and now we can build our solutions to protect them. And 75% of the Fortune 500 companies trust us to help them improve their security of their business. You know, over the last 20 years, we've seen a shift in the prioritization of security, and no longer is the CISO, the chief information security officer, our only client. Our clients are now the business unit leaders, the chief risk officers, plant managers, product managers of cars, store managers, and all the members of the C-suite. Security is top of mind and spreads all across the organizations. As a matter fact, just yesterday I was meeting with a CEO, talking about cyber risk to his electric company. So in summary, security is everyone's business, which means you. For us at Accenture and in our personal lives, and certainly for our clients, I hope you learn a lot from TQ materials that we pull together. And so there's a lot to learn about security, so grow your TQ, grow your impact, and happy learning.

Security: Executive Briefing

Introduction

In the early years of computing, security often wasn't much more than having a lock on the data center or asking people to change their passwords once a year. So, yes, things have changed quite a bit. Today, the word information security, and some people use other terms, like InfoSec or cybersecurity, but for our purposes, we're talking about the same thing. To think about all aspects of computer systems, from the physical hardware, computers, networks, all the devices connected to those networks, not just laptops and phones, but these days, we're also talking about alarm systems and cameras and door locks and thermostats, the different software applications that all of these devices run, and, of course, huge amounts of data, intellectual property, customer information, documents, databases, emails. Securing all of this is a critical and ongoing task for every organization with a direct impact on your bottom line and your ability to be agile in the market. So to be clear, what we're about to cover will not just be a few typical personal security recommendations like you should have strong passwords or use two-factor authentication. Yes, that's important. But our focus here is security at the organization level, the different ways this impacts the companies that you work for, the projects that you're a part of, and the teams that you work with. We will begin by taking this vague idea of security and breaking it into more useful specific areas, several functions that work together mitigating different risks to your organization and combining to form the suit of armor that protects it. Any gaps in these business functions represent different types of vulnerabilities that open you up to various threats. As we talk about how to close these gaps, we'll go over some security terminology and jargon, and there are a few terms that you've probably heard of already. But there are others that might be new to you because, yes, like everything else in technology, the security landscape is always changing. There are always new kinds of attacks, new vulnerabilities that malicious actors will try to discover and exploit. But whatever your role is, you can be actively involved with this without needing to become a security expert because over the last few years a lot of work has been done to develop principles and best practices. We have structured repeatable, cost-effective approaches to plan and think about security. They'll bring our attention to different aspects, make sure that we avoid any blind spots, and, in some cases, even just allow us to have meaningful conversations about it to make us and the organizations that we work with better protected and less vulnerable. Welcome to the Executive Briefing on Security.

The Threat Landscape

Okay, nobody will disagree with the idea that security is important, but they will disagree about what that means. They'll even argue about what the most significant security threat actually is. And it's easy to get the wrong idea about this. When you hear about businesses being hacked, those high-profile attacks that make the evening news, often there's a common theme. The personal data of over 50 million customers was leaked onto the internet after one of the worst hacks in corporate history. Hotel company revealed that this recent attack on its computer systems has compromised the data of 400 million users, including credit card and passport information. This latest cyberattack has exposed the confidential information of over 100 million customers. Were you affected? Tell us how you feel. Call in at 1-805-555... It's very easy to see these and think to yourself, Clearly, the main focus of security is to stop hackers from stealing our customer data. I have a full understanding of this, but being over-focused on one potential threat or what we call on attack vector can distract us from the many others that are often far less dramatic, less newsworthy, but just as significant. Many security risks are simple. They're mundane and, honestly, kind of boring. For example, a disgruntled employee on their last day accesses an internal server and deletes or corrupts a bunch of internal project planning documents and data. You would not see this making the news. There was no hack. There was no leak. Your customers data was unaffected, but it can be just as impactful to your business. Some vulnerabilities are external, but many are internal. And even if attacks do come from the outside, they won't have the singular focus on getting your customer data. Today's attackers have a wide range of motives that go well beyond that. Some try to make money through ransomware to install software that will effectively lock down a computer and everything on it and only unlock when you pay them. If this software gets onto your laptop or your desktop, it's for sure a major inconvenience. But if it gets onto the server that hosts your website or holds your corporate database, that's a whole nother level of pain. But other attackers aren't looking for money, but instead will take a business offline to make a political point, sometimes called hacktivism. Others don't care about obtaining your customer data. They're looking for your intellectual property to corrupt the data that you use to make decisions or just to gain a back door to your systems so that they can quietly hang around and spy on your operations to gain an advantage. And some attackers don't have any goal at all other than to just generally disrupt a business, any business, because they can. Or, worst of all, other malicious actors are looking for ways to leverage cyberattacks to cause physical, real-world harm, destruction of property or loss of life. And no one is too large or too small to be a target. It's not unusual for an organization to be complacent and assume that, if they don't have a big public profile or if they are a smaller business, that no one will be interested in targeting their computer systems. But that's not the right perspective because many attacks are basically random and opportunistic. They're the equivalent of a thief walking along the street, quietly, testing the door knobs. They didn't set out on a target of one specific house. They're just looking for any vulnerable house to exploit. So we need a way to bring our attention to all of the different areas of focus, the different types of security risks and vulnerabilities. If we're talking about security, what does that mean? And what is it that we're trying to secure? And, luckily, there is a simple shortcut, one small word that's been around since the 1970s to help us do this.

The CIA Triad

For several decades, we've used a simple abbreviation to explain three overall goals of security. C.I.A, and no, not the U. S. Central Intelligence Agency. Here, C.I.A a stands for Confidentiality, Integrity and Availability. It sounds almost too simple, doesn't it? Just three words, but we use this to help us evaluate the data, and IT functions most critical to the operation and success of organization, or even one specific project within that organization. Let me walk you through what that means. Confidentiality is making sure business systems and data are only accessible to the right entities. And I use the word entities because this can mean people, employees, contractors, business partners, but it can also mean other technology systems. Our HR system needs to talk to their payroll system. Their website needs access to our inventory database, but still we need to keep our secrets, well, secret, and share information we want to share only with those that we intend to share it with. And when an organization is unable to keep personal information confidential, it can cost millions, in some cases, hundreds of millions. Integrity is about making sure your systems and data are what they're supposed to be, that we can trust the information is accurate. We can trust everything is current up to the moment, and that there's no corruption. Nothing's been added, or changed, or deleted, and in some situations, manipulation of trusted data I can cost not just dollars, but lives. Think of computer systems that run power plants, or emergency service dispatch, or air traffic control, that data has to be accurate all of the time and trusted, or people's lives are at stake. And availability is about making sure your systems and data are online whenever they're needed, accessible from the right locations, not just ensuring that internal systems are up and running, but also that there's nothing outside interfering with anyone's ability to reach us. As a simple example, if your organization has a customer-facing website selling products or services, every second that site is not available. Is money lost. So all three goals are important, and I'll say that again. all three of these goals are important, but they're not equal, and you can find them prioritized in slightly different ways from organization to organization and even project to project because all of them have a financial impact on organizational cost, and improving one aspect does not always help the others. As just one example, if you decide confidentiality is the single most important factor, you might make decisions that downgrade the availability by only allowing access at certain times or restricting connections from some locations. But with these three ideas in mind, we can drive a little deeper into the different aspects of security that make up your overall risk mitigation strategy. But a quick sidebar, while security today is an immense, multifaceted topic, I will say again, you do not have to become a security expert to engage with this. And here's what I mean. If I'm a homeowner and talking with my next door neighbor, we can have a conversation about the importance of a good lock on the front door, and neither of us need to be a locksmith. If we see cracked tiles on the roof, we can understand how it can make it vulnerable. We can recognize drainage issues or see exposed wood as a risk factor for certain pests. And sure, sometimes we may bring in experts, but it's completely possible to understand and recognize common issues, plan for, and even implement solutions without requiring deep technical knowledge. But let's keep this homeowner analogy going a few more seconds. If you've ever done any modest home renovation, you know how quickly your to-do list will become overwhelming if you don't start to categorize all the different things that need to be done. You might group these tasks room by room. Here is the list of things that we need to do in the kitchen, and here's the list of things that we need to do in the bathroom. Or you might not go room by room, but instead break it into different aspect. Here's all the electrical stuff that we need to do, here's the plumbing work that we need, the cosmetic list versus these structural alterations, here's the ongoing maintenance tasks, and so on, and so on. And however you choose to categorize tasks, there's always some crossover in dependencies, but still, breaking them into different areas of focus make it easier to think about, plan for, and achieve, and it's the same here. So while there are many different ways that you can organize the elements of security, we're going to break it into six areas, and we'll go over each one to explore what value it brings to the business, or, in many cases, what value it protects. We'll begin by looking at the security of various products we build and use, and this includes software applications and infrastructure. We'll then shift our focus to access management, controlling who can get to our systems and what they're allowed to do. After that, we'll cover specific issues for securing our data and ever increasing focus for almost all organizations. That will lead us to governance, where we'll also touch on risk management and compliance. Understanding those first four will help us in exploring security operations, which includes secure administration. Finally is cyber intelligence and testin, a key component of a mature cyber defense and a distinct important element for your overall security plan. So let's get started.

Sidebar - Hackers And Actors

A quick sidebar. In movies and TV, if you have a character who attacks or compromises a computer system, they're usually called a hacker. Nowadays, it's universally been morphed into a term to represent a villain, and they're surprisingly easy to recognize. They always seem to wear a hoodie. They work alone sitting in a dark room furiously typing green text on a black background. The reality, of course, is not so simplistic. Compromising a computer system doesn't have a dress code, and it's rarely about how fast someone can type. Even the word "hacker" is problematic. It has a long history and not all of it's negative. Describing something as a hack can mean just a quick and dirty fix, a clever solution, not necessarily an attack. So in the security community, while hacker is, of course, understood these days, it's more common to use threat actor or a malicious actor instead. It's more clear and more intentional usage. And threat actor or malicious actor can mean an individual, but it can also mean an organized group, whether that's a criminal group or even a state-sponsored organization, called nation state actors. So we'll mostly use those terms moving forward. End sidebar.

Product Security

We'll begin by talking about the area that a lot of people have in mind when the word security comes up. Product security is about making sure any products that you build and/or use, including software, are designed to be as secure as possible. And this focus doesn't just look at products we develop in house, but also the commercial software that you have paid for and implemented and infrastructure and platforms that your software runs on. If you've heard the term application security, which is identifying and fixing security vulnerabilities in your own software applications, that's part of this larger product security story. As you purchase, install, or develop any new system, whether it's part of your own infrastructure, a new software application, or a product that you are prepping for market, it should be securely designed from the outset, following current industry best practices and including security specialists in the process. This is the time that you want to bring in the experts. They're the ones who know what you're up against, and they can help you make sure your new systems have the best possible chance of being secure from the start. And even if your developers have secure coding policies and best practices, we recognize that they aren't static and must continually evolve as we learn of new and emerging trends, vulnerabilities, and exploits. And this means your development teams need to be continually learning and growing their skills as well. This includes your infrastructure teams too. Their skills need to continually evolve to maintain a secure infrastructure over time. So what are these security best practices when it comes to building and using applications and infrastructure? Well, and this is a very common answer to questions about security, it really depends. For example, the best practices to build a more secure on-premises infrastructure where you own and control all of the hardware are different from those that you'd use when outsourcing parts of it to a cloud provider. And security best practices differ based on the kind of software, web applications, mobile apps, and desktop apps that all have their own specific issues, and between programming languages as well because there are technical implications of how different languages are implemented on different infrastructure. The point is to be looped into the industry best practices that apply to the specific technology that you are using and then expand on those within your teams to meet your specific needs and to mitigate the specific threats that your organization may face. But that same dedication needs to go to your existing systems, conduct security reviews, and decide what security concerns might exist and how you can mitigate them. If you've had a system running for five years, it may have been secure back when it was first implemented, but you need to continually review infrastructure, code, and more to make sure that it's prepared to deal with today's threat. You also need to implement policies and practices that help mitigate the risk to older systems, such as controlling who can access them, from where they can be accessed, as well as implementing monitoring capabilities for vulnerabilities that you can't patch because some of these can't be patched in these older systems or they will break the application. And I'll keep coming back to one idea. Security is a continually moving target. It's something that has to be part of the day-to-day routine for every part of your technology estate. Whenever you decide to build or implement a new system of some kind, just be aware that you're making a long-term permanent commitment to keeping that system secure as the threat landscape evolves and changes. Your organization likely uses enterprise software platforms that you buy or lease from someone else, SAP, Oracle, Salesforce, Workday, you name it. You need to understand how those systems are secured. More importantly, you need to understand what elements of security will be covered by the vendor and what elements of security will not. These days, it's common to see a security responsibility matrix for cloud providers to make it very explicit what they take responsibility for, like the physical data center and the machines themselves, versus what they expect the client to handle, like users and account management. Your team needs to understand how to harden those systems against attack, how to monitor them, just like you would monitor your own assets, and when it comes to products, software, and infrastructure, the thing to remember is that nothing is secure forever. Systems are updated, configured, and developed in real time, and with each change, you are creating the potential for a new vulnerability. There are teams of people, both benevolent and malicious, poking and prodding at hardware and software systems alike looking for vulnerabilities and creating exploits. I myself am occasionally one of those people depending on the hat that I'm wearing. So even when nothing is being changed, old systems become vulnerable as new vulnerabilities are found. Part of any organization's core competency needs to be keeping their systems, both the ones that they build and the ones that they buy, capable of dealing with the modern threat environment.

Identity and Access Management

Identity and access management, often shortened to IAM, is part of security that deals with two simple but incredibly important questions. First, who are you? And second, what are you allowed to do? We begin with identity. These are the mechanisms that you have to have to define and validate who's who in your organization. These might be a single directory users log into to prove who they are, or it might be multiple different directories that authenticate users for specific purposes. But there's more to identity management than just creating user accounts and making people change their passwords. We recognize that there are different types of identity, ways to represent employees or devices, partners, contractors, or other software systems. But nothing in the business world is static, so beyond the process to create accounts, you also need processes to regularly review all accounts and make sure that they're still needed, because a neglected or orphaned account that still has access is a really great way for a malicious actor to gain entry to your systems. Some of these processes can be automated, like automatically removing a contractor whose contract has ended. Or they might be part of a larger process, like when an employee leaves the organization, or maybe even something that's manual from doing a periodic review. But there are important aspects beyond just is this account active or is it not? For example, if we have an employee based in Iowa but their credentials are suddenly being used to log in at 3:00 am from halfway across the world, that might be legitimate, but it could indicate that their account has been compromised and someone is attempting to impersonate them. This kind of situation is something that your systems should automatically be raising as an alert, and where you would have someone to receive that alert and quickly look into that situation, and that's exactly what security operations centers are for, which is something that we'll get into in a few minutes. But even when you can confidently match real-world entities like employees to an account and validate their identity, there's the separate issue of maintaining what they should have access to. If we create an account for a new employee and they successfully logged on, that does not mean that they should instantly be able to change the home web page of our website and delete all of our databases and then access the payroll system and make themselves the CEO. There are multiple levels of permissions and privileges, even when someone's proven their identity. And just like identity has a lifecycle, what the identity has access to also has a lifecycle. If someone needs to use a system, does that always mean forever or until the job role changes? Or do they just need it for a month, or just a day, or maybe just an hour? There's a security guideline called the principle of least privilege, that wherever possible any user account should only have the absolute minimum permissions necessary to complete the current task. And this doesn't just apply to entry-level employees. In fact, it's more important for advanced administrator roles. Many organizations have a separate set of elevated administrative privileges with access to the most critical assets in the organization. And one bad apple can subvert your entire system, so it's important to closely limit the scope of what an administrator can do at any moment. So smart organizations have processes that remove most capabilities from their administrators' users accounts. And when an admin needs to do something advanced, they use special tools to temporarily request elevated permissions, and when they do that, it will trigger an alert to log that request. In normal use, the security systems will ignore that alert because the action is part of the admin's normal job. It's part of their behavioral baseline. However, if it occurs too frequently over a given period of time, it might indicate a problem that someone should look into. But most of the time the admin can finish the task they are performing, and their elevated privileges will be automatically downgraded. They're able to do their job but in a controlled and monitored fashion that keeps everybody safe. If that seems like a lot of work, well, it really is. And that's why many organizations use access management tools to help automate that work. With the right tools and skilled people to implement them, you can create an actively secure environment without creating a lot of manual repetitive work for your teams. Identity and access management are the foundation for everything else that your security plans are built on, and so it's important to take the time to do them right.

Data Security

Today's businesses accumulate an incredible amount of data and not just the usual suspects like customer addresses and order information. We have data gathered from advertising campaigns, customer behavior, and these days, data generated by machine learning, artificial intelligence systems. Beyond that, there's company financial and operational data, legal data, proprietary engineering designs, and the list goes on and on and on. Whatever you have, it's your most valuable intellectual property, your competitive edge, hence, the security of your data that's paramount. Companies need to have a plan for securing data, and you can break that plan down into three basic elements. We start by securing data at rest, wherever it's actually stored. And this might be on your own on-premises servers, but it also might be in a cloud provider. It might be data in an electronic document, or it might be in a database, any of your data, no matter where it is stored and no matter what form that it's in. We think about how this at-rest data is protected from accidental or unauthorized disclosure, even protected from physical theft. So, first, we need that well-defined identity and access management that we just talked about earlier. But on top of that, we can also implement encryption so that even if other layers of security fail and the stored data is stolen, the data is encrypted and not usable, and we have effectively mitigated that security threat. This concept of multiple layers of failsafes is described as defense in depth. Next, we think about how the data is protected when it's in transit, being communicated from one place to another. Again, various types of encryptions are used to make sure that data in transit isn't seen or modified by anyone else. And, finally, one thing people often forget about is the security of data that we've generated or received from someone else or someplace else. Can that data be trusted? Did we receive it in a way that's secure so that we can verify it wasn't tampered with? We're likely making business decisions with that data, so we want to know where it came from and where it has been. Another way to think about these three elements is, Where is our data? Where did our data come from? And where is our data going? Making sure that you have a plan to provide the right level of security in each case is the key to an effective data security program. Data really is the lifeblood of your company. You can imagine how important it is to make sure that your data is not only protected but also trustworthy. Smart businesses make all of their big decisions based on their data and information, and you want to ensure that you're operating from a safe, secure place when you do so.

Governance

Most organizations use the words governance, risk management, and compliance to refer to distinctive activities that each have specific goals and outcomes. In practice though, they're quite interrelated, and some businesses use terms like GRC or integrated risk management to cover all of them. First, let's talk about governance. This is one of those words that you see used in politics and corporations, land management, healthcare, and it can seem a bit ambiguous and vague. In the context of security, governance describes how we formalize those strategic high-level responsibilities, policies, and procedures around security efforts. And while there are specific low-level security techniques and practices your developers and administrators need to focus on, governance describes the higher-level decisions to drive your security goals. How do you ensure your overall security approach stays intact and relevant in the hustle and bustle of day-to-day business? How do you decide on security priorities and share information across teams? What processes and procedures are in place to ensure that security won't be forgotten in a moment of pressure? Governance also includes understanding the evolving threats that your organization faces and developing plans to mitigate them. It even includes the human side of security, such as establishing policies that direct employees, contractors, and others to take the best approaches to staying safe. So now let's look at risk management. This is a big part of any effective security plan, and it's not just about identifying the risk that your company faces; it's about weighing those risks against the cost of mitigating them. Think about it this way. It is easy to achieve complete security. Just shut off all your computers, unplug them, and go home. That will keep everything secure, but it won't really make for a very effective business model, will it? So risk management is not about preventing every possible risk. We can't do that. What we can do is evaluate the risk from plausible threats and assess the potential business impact. The result is either a qualitative or even more detailed quantitative value that serves as the basis for a level of security applied to mitigate the risk, or in some cases to offset the risk by transferring it to a third party like a cyber-insurance company or a managed security provider. It's about understanding the risk and managing it to whatever degree the business requires. And for many companies, that takes us into the realm of compliance, which typically means the need to demonstrably conform to some external security requirements, like laws or regulations. These vary significantly by region and business function, but examples include the European Union's General Data Privacy Regulation, or GDPR, or in the US, the HIPAA security rules for healthcare information. Your risk management activities will be based in part on the compliance that you're required to meet, and your governance activities will need to take those into account on an everyday basis. That includes not just securing your data but maintaining that security and being able to report adherence on an ongoing basis as well. And how do you know that you're doing all the right things when it comes to risk management in governance and compliance? One way is to partner with a respected consulting firm. Most of them have created assessment models that let them review an organization and determine if they're seeing the right kinds of activities and processes happening. It's like a second set of eyes filling out a scorecard. They let you know when you're doing the right things, and they let you know when you have room to improve.

Secure Ops

In this section, what we're calling Security Operations will cover two topics. First, there's secure administration. This is really just your ordinary IT operations team doing their job every day with a firm focus on security at all times. They're managing your servers, administrating your network and other infrastructure, deploying applications, backing up the email server, and everything else that they do every day, all done with the firm awareness on the importance of security in every action. You can't underestimate the role that secure administration plays in your total security picture. Everything from making sure that only the right systems and the right devices can attach to your network to ensuring that those fancy smart light bulbs are updated and secure all falls under secure administration and operations. It's a lot of work, and it goes on every single day. Then there's the dedicated set of activities, often handled by a SOC, or security operations center. These individuals are the moment-to-moment operators of your dedicated security activities. They're the ones watching your entire environment moment to moment and responding to incidents. They are the (alarm goes off) hold on a second. Excuse me. Speaking of incidents, yeah, okay. I think we're good. Looks like our security operations center is already on it. But that's exactly what I'm talking about. We registered some unusual activity, a potential security problem. And our systems are configured to send alerts, but someone has to see those alerts and respond to them, which is what they're doing right now. It could be anything from an administrator suddenly resetting a lot of account passwords or an application seeing an unusual number of logins from an unusual location or, well, really, just anything. And, you know, this is a really good example of how some of the major pieces of security fit together. For a lot of organizations, it starts with activities like software development, one of the places where new technologies and systems come to life. A software dev team focused on security might make sure their app does things like run security self-tests before it starts and making sure the application is instrumented to send activity events to a central location. The operations team works to ensure the infrastructure is secure, and that might include making sure a central location is available for all those events and alerts to be sent to. And the security operations center receives and responds to those events and alerts deciding if something is a security problem, and if it is, handling it. You've probably heard of this term, DevOps, which, to use a really short definition, means the developers and operations individuals and the organization working closely together to put applications into production. But that trend is now actually going a step further to DevSecOps, which pulls in the security teams in the loop from the outset. The idea is to create and deploy technologies that are easily secured right from the start, and to make sure both operations and security operations teams have what they need to do their jobs effectively. It's a great way to make sure that you're not only building secure systems, but that you're building systems that are designed to be monitored and kept secure over the long haul. But as well as the day-to-day operational procedures, we should also have procedures in place for our response to any security incident. How do you conduct postmortems after an incident? How do you measure the impact of the incident on the business, make sure any fixes applied will work, and ensure the same thing can't happen again? And this leads us into cyber defense.

Cyber Intelligence

Finally is cyber intelligence and testing. It's all about how your organization prepares to combat specific threats and what processes you have in place to deploy those defenses when the need arises. It's about your resiliency in the face of attack. Some organizations roll their cyber defense activities into an existing area of their org chart, and that's fine. Others build a special team on the org chart to handle these tasks, and that's fine, too. What's important is to recognize that these activities provide specific and unique value to the businesses and that they need to be things that you do all the time continuously in conjunction with the other security functions. Let's start with threat intelligence. This is how your business knows on the day-to-day basis what you're up against, what's going on in the world, and how it might affect you. Was there something in the news that might cause your specific business to become a target for hackers or for people looking to make a public statement? What new attacks like ransomware or malware are suddenly in circulation? This means keeping an eye on the news, on industry reports, and more, all on the ongoing basis. Penetration testing, or pen testing, is another important activity. This is where people deliberately try to gain access to your systems and data without authorization.

They try to find the holes in your security so that you can patch them before a real threat actor gets in. These people might be working for you, or they might be consultants that you hire. They're generally interested in testing your actual technology systems, which is an important part of a strong defense. A step up from pen testing is the idea of red teams and red team operations against blue teams, which tends to be a more holistic activity. The red team role, often performed by trusted outside consultants, pretends to be an actual threat actor. Like a pen tester, they're trying to gain access to your systems. But unlike a pen tester, they'll try to use every dirty trick that the actual adversary would and proceed past your external boundary to have persistent post-exploitation operation. This allows for your defense to be tested over a longer period of time and focus on achieving specific outcomes or actions on their objectives following the full lifecycle of an attack. The idea is to expose the holes wherever they may exist in your organization so that they can be fixed. They may try to use social engineering against the people in your company. Let me show you how that works. Social engineering isn't a technology. Quite the opposite. It's low tech, even what some would call no tech. It's using psychological ways to get information from people or to get them to do something. This includes phishing emails or text messages, even something as basic as just phoning some random employee at the company and saying, Hey, hey, it's Bob from tech support. Yeah, yeah, we're running a security audit. Oh, I know. It's always something from us, right? Hey, look, could you tell me what you're currently using as a password? Uh huh. Yeah. Uppercase P? Oh, is that your cat's name? Oh, that's adorable. Yeah, yeah, that's great. Thank you so much. You're good to go. And thanks again. Have a great day. Yeah, yeah, you too. You might be surprised at just how often that can work. And a red team will do those kinds of things, testing not only your technical defenses but also your processes and procedures and people. A red team can work entirely on their own, just like an organized adversary would. Sometimes, though, you might want to run scheduled red team versus blue team exercises where your own security staff, they're the blue team, actively responds to the red team, cuts off their access, mitigates the red team's threat, and so on. It really becomes kind of a cyber knife fight. It's a great way to test not only your technology but also your processes and procedures and, most importantly, your people. An organization's approach to security, that is, the specific tools that they use, the actions they take, and the processes that they use, will always be changing. After a red team test, for example, you may modify your processes or engage in different kinds of security training for your teams based on the results. After an actual incident, you will conduct a postmortem to consider permanent mitigations for whatever permitted the instance to occur, also known as the root cause. You will engage in threat modeling to test your implementations and create confidence that they're actually effective. It's always an evolving process, anticipating and responding to whatever the world throws at you. Many organizations will appoint a dedicated Chief Information Security Officer, or CISO, to oversee these specialized cyber defense efforts, along with all of their other security-related efforts as well. Some organizations will rely on a trusted consulting partner to provide these services, and still others will put these efforts directly under the CEO or another executive. But wherever these functions fit in the org chart, you hopefully can see the importance of cyber defense as part of a complete security plan. And let's be clear, a security plan is a mandatory part of any modern organization. It's a way to provide executive level direction that embeds security practices throughout the organization, making security everyone's job.

Summary

We've covered a lot at a high level. We've looked at product security, identity access management, data security, governance, security operations in cyber defense. As you've seen, there's a lot going on with security in our modern world. Organizations need to understand the risks and implement not only appropriate safeguards but also implement ongoing processes into organizational investments, as well as executive-level sponsorship to mitigate those risks. And, remember, it's all about CIA, confidentiality, integrity, and availability. Security is a space every bit as complex and robust as finance, legal, human resources, or any other part of the organization. And at this point, you should have a better idea of what security looks like in the organization, how to think about it, and how it supports the business over the long haul. Thank you for joining me.

TQ Security Aftershow

What is Security

When I say the word security, how do you feel? A bit anxious? Maybe even a little bit intimidated? Does it make you feel safe? Or maybe stories of data breaches and identity theft go through your mind. Well, on today's show from our virtual TQ HQ, we're diving into the topic of security. It's an important topic for our company, for our clients, and for each of us as individuals. But spoiler alert, it doesn't have to be confusing or intimidating, so get ready to feel safe, comfortable, and secure as we explore the topic of security on this edition of the TQ Aftershow. Welcome to the virtual TQ HQ. -Hey, Kelly, thanks for joining me today. -Hey, Sarah, thanks for having me. How much time do we have today? Because, you know, once I get started talking about security, it can be really hard to get me to stop. -I know, I love to talk about security, too, but let's just start with 30 minutes and and see where we go. And for those of you who are joining us and don't know Kelly Bissell, Kelly is our global Accenture Security Group Lead, and today he's my co-host on the TQ Aftershow. So at Accenture, we believe the world's best security experts are on our side. And lucky for us today, we have several of them joining us. We want to explore what security really means for Accenture, how we protect ourselves, and our clients, and why security is important to everyone. All of us, not just our top executives. And as always, we're going to bust some serious myths about security. So let's welcome Accenture Security leads. We have Neha Joshi our Accenture Securities Growth and Strategy and Innovation Lead. Ryan LaSalle, our North America Security Lead. And Paulo Dal Cin, our Europe Security Lead. Neha, Ryan, Paulo, thanks for joining us today. -Hi, Sarah. Thank you. -It's great to be here. -Hello, hi, thanks. -All right, thank you all. Kelly we're just going to dive right in because we have a lot to talk about today, but let's break it down a little bit for our audience. Maybe you could start with how we think about security at Accenture. It's about protecting ourselves and our clients, but maybe a good way to think about it is, we're really all trying to not become the next big headline, right? -Well, yes, to an extent. But of course, there's a lot more that goes into that. You're right. There have been a ton of cyber breaches over the years. In fact, 50% of the companies have had incidents where a lack of trust impacted their reputation. And, as you guessed, that can have a tremendous impact on their business, their stock price, their earnings, their profitability. But to be clear, our security practice helps clients thrive and innovate safely. So you asked me to break it down, so let's do that. First of all Accenture Security, our goal is to secure the world for our clients. I know, I know, it sounds like a lofty task, but we're committed to two really major points. One, for our clients. We want them to look for us to solve their most complex cyber challenges. You know, we do that through innovation and through our global experience, and are super deep industry expertise. The second thing is around our people. We're invested in training to build that next generation of security, by enabling them to have a place where they can learn the best and grow their own career. We want them to know that Accenture's the place that they can shape their own future to be the best. We have the very best people at Accenture, and I'm really proud of that. They're equipped to solve those complex problems across all industries. Well, let's take a couple of examples, if that's all right. The leaders in healthcare industry have a focus around protecting patient data, making sure their records are safe and private. But at the same time, they're trying to find new ways to make advancements in that digital health area. So how can they keep their patients healthy and their data private at a lower cost? That's where we come in. All the innovation that we do helps them achieve that goal. But these goals are different for clients at a banking institution, where they're focused on ensuring that they have protections in place to avoid account fraud and new developments with crypto currency, like Bitcoin. And so the goals at a bank are different from a goal at a healthcare company. So it depends on the industry and the specific problems that they're trying to solve, even though the goals are similar. So we want to ensure that the platforms that house their data are secure, and any new tools and applications that they create have the same security. So it's the intersection between our wide security capabilities and our deep industry expertise that allow us to deliver solutions that can really help our clients be safe and we can secure the world. -Yeah, I love it. Those intersections and balancing those priorities, being innovative but still being secure and all of the different priorities that the different industries have, quite a complex problem that we do have. And I love that idea of securing the world here at Accenture. So we do have amazing people at Accenture with the right skills. It almost brings to mind an image of all of our Accenture people wearing superhero capes, like in a Marvel movie getting ready to go to battle. Whoa, whoa, whoa. What is that? -Cash are you in? -Roger that, Tango. May it be loud and clear, and I think we did it. -Mission accomplished. We have achieved hacking nirvana and infiltrated the TQ Aftershow. -Okay. Okay. Wait a minute here. I'm not sure what's happening, but I think, is that Bob and Brian trying to hack into our aftershow? -Man! -Uh, no, Sarah. We're Tango and Cash. -Yeah. -We hacked into the aftershow. We're in transmission. -Okay. Okay, everybody, calm down. Well, I appreciate the spirit here. We have not been hacked. You're protected by some of the best in our security group. And we're all connected on an Accenture approved platform. We're all on a secure connection. -Okay. Kelly's right. We didn't actually hack in. -Yeah, Brian and I are trying to do kind of a backdoor audition into hacker land. Like I'm thinking I could be the next Treasure and he could be the next Queenie, and it would be really, really awesome. -Yeah, and Paul Daugherty did ask us to drop by and just remind everyone, you need to stay vigilant. You never know when a hacker will occur and what to do. -Well, I'm glad we got that cleared up, and thanks to Paul for helping us make that point. I was about three seconds from dialing up ASOC. So, Kelly, maybe your team really are the superheroes of Accenture when we have to fight off hackers. So, nice try Tango and Cash, or should I say Bob and Brian? And can you guys please stop trying to get on these aftershows?

Our Role and Security Offerings

-Okay, sorry about that, guys, but it does bring up a great point, and it reminds me of Hackerland, which I know is a widely-popular show here at Accenture. I think it's probably what a lot of our viewers associate with security across Accenture, but let's talk about that a bit. We've got the Information Security group at Accenture, which is a different team from the Accenture Security Team, right? -Well, it depends how you look at it. So we're all Accenture people committed to keeping our clients secure. Our Information Security team make sure that our own Accenture information, people, and systems are secure through training, technology, and the Client Data Protection program. They help all of us to reduce the likelihood that we inadvertently introduce a security incident during a client delivery. For Kelly, Ryan, Paolo, and myself, and the rest of the Accenture Security practice, we're helping our clients protect their own information, people, and systems. We can do that through advisory, transformation, or operations engagements, and it's important for us in the security practice to be knowledgeable about what we do at Accenture to keep ourselves safe because our clients want to make sure that they are doing business with a partner that's safe themselves. So we work together very closely advising on Accenture Security position and supporting their deployments and operations. -Yeah, okay, so it's a great way to look at it, and honestly, being in CIO, it reminds me a lot of what we do in CIO, where we focus on our internal technology and we have, you know, our practices out in Accenture that are focusing on our client's technology. So our Accenture Security Group and our Internal Information Security group, they have the same goals, but they approach the problem a little bit differently, where Internal team looks at what we do to protect Accenture, and Accenture Security focuses on helping our clients protect themselves. I think that makes a lot of sense. But, Neha, you said earlier that our clients, you know, they play across a lot of industries, and they have unique needs, so how can we, at Accenture Security, really bring a value to fit all those different needs? -Yeah, great question. So, as you mentioned earlier, our security practice has been around for over 20 years, and over that time, we've exploded with growth of more people, more capabilities, and more offerings to protect against the growing threat landscape because that also was growing over those 20 years, right? Our practice is really built around three main services, where we believe that we can deliver the most value to our clients. The first is Cyber Defense, and our capabilities here allow us to advise our clients on how secure they really are today. So this is like the cool stuff that you think of where we can actually simulate attacks against our clients, to see how their own current processes and tools will respond to protect them. We can also dig deep into how they run security today, and recommend you tools and technologies that may reduce the time it takes them to detect and respond to threats in the future. Applied Cybersecurity is our second service, and this is where we transform our client's technology programs securely. So our clients that manage a lot of sensitive data like banks, for example, may need our data security capability to implement new technologies to better protect, control, and analyze that data, or a client may want to move their entire organization to the cloud. Well, our cloud infrastructure security capability can help them to do that more securely. The last, but not least service is Managed Security. This is where Accenture manages the cybersecurity operations for our clients, so we can continuously detect and then respond to threats across an entire client's organization to minimize the impacts to their system and to their data. When we can manage the security operations on behalf of our clients, we can find ways to innovate, to allow them to be stronger against those biggest, the biggest risks that are facing them. Now in addition to these three core services, Sarah, we also have specific solutions to the industries that we most commonly serve because as we said earlier, every industry needs security, but every industry is unique. So, for example, our products clients may have physical security needs for stores and for customers that we don't see in other industries, our financial services clients must adhere to a lot of regulations and and often look to us for advisory support on how to quickly respond. We also offer operational technology security services to connect devices to existing systems to secure products, and services, and and even oil rigs, not only for our clients, but for our client's end users. Our strategy and risk services partner with board of directors and C-Suites to redefine security programs and long-term strategies, so that they could be more effective and proactive for the future. So you can see that we do a lot. -Yeah, there's a lot there, and it's actually great that we're talking about security because I feel like in almost every TQ Aftershow that we've had, whether we've talked about cloud or data, security is one of the main topics that comes up. So this is great to understand how we have this practice that addresses all of these issues and a lot of them that we haven't even talked about before. It really is amazing, the depth and the breadth of the services that we have. -So Paolo, the services we offer in cyber defense sound pretty cool. Maybe you can help our learners understand what we do for our clients. Like, how do we simulate attacks through penetration testing? -Sure, Sarah, it's a very nice offering. So, one of the key initiatives of any security program is trying to outsmart the attackers, ensuring that you are just not one, but many steps ahead of them, which means that we need also to have people on our side that think and act like attackers. So penetration testing, also known as the ethical hacking, is a way to simulate cyberattacks in order to test the security level of companies and organizations. In other words it's trying to intentionally hack into the computer systems and networks, exploiting their vulnerability. Think a little about adding good guys hacking in the system before bad guys, we try to do so. So let me also try to share some great example of what our Red Team has done in the past, obviously with our client permission because it's a very important activity. So first of all, we were able to wire money out of the banks, second, cash in at a casino with the fake tickets, but we were able also to access patient records of healthcare providers, or to unlock a car without having the key, or broke in tow air traffic control system without any authorization. So if those kind of things were able to be done by the wrong people, it could be a disaster for client business. So, please remember that one in three attack attempts are successful, so it's very important for our client to understand where they need to have a better security posture and improve the security level, and improve also the defense capability. -Yeah, wow, that is really amazing and actually quite scary, all of those things that we've been able to do, but as you said, good that we have the good guys doing it before the bad guys do it, and the examples that you gave, Paolo, it really brings the light that almost every business that we use every day can be vulnerable. So, I think many times we kind of take it for granted that our information is secure and that the business we interact with is trusted, but there's a lot going on behind the scenes to ensure that that is in place.

Cyber Fusion Centers and Accelerators

-So hearing all of you speak, it seems like our security practice is pretty mature. I mean even though, Neha, as you said earlier, security has really become a really hot topic and is really coming to the forefront in recent years. -Yeah, our security practice has actually been around for over two decades. So Accenture actually started taking security seriously long before it was cool, or most people even realized they needed it, right, and because of our deep history and our experience, we're actually able to do a lot of great innovations in the security area with our clients, and we're actually able to showcase them at our Cyber Fusion Centers. That becomes one of our key differentiators for our client. -Yeah, I guess I didn't realize, like you said, it seems like nowadays everyone realizes security is important, but we've been at it for quite a long time. And these Cyber Fusion Centers, those sound pretty cool. So, Ryan, can you talk to us a little bit about what we're doing there? -Sure thing, Sarah. Our seven Cyber Fusion Centers, each have its own unique personality, but they share a common formula. They all bring together a unique mix of talent, disciplines, and client experiences. For example, our Cyber Fusion Center in Prague brings together security hunting and monitoring teams with those offensive teams that Paolo talked about, along with our automotive and embedded systems security testing labs, and that brings together a full circle of capabilities for our clients. We can help them find new vulnerabilities, demonstrate the impact when those things are exploited, create the manage defenses that actually protect them, and then exercise them to see if they're actually up to snuff. That team recently actually found and disclosed to the vendor a series of really creative vulnerabilities in a major automotive manufacturer's product line. Other Cyber Fusion Centers bring together innovation and operations, or they merge cyber threat intelligence with incident response and research and development, or they go really deep into one of those industry value chains that's important to our clients, like energy or manufacturing, where we can fuse capabilities like intelligence, engineering, and operations together to help them be more effective. But all of them have a set of really innovative client experiences. These are great places to go even virtually to help bring together a picture for our clients of the journey they're about to go under and how to get there using innovation to drive better outcomes. One of the lessons that Kelly's talked about is that no matter what we're doing for our client, whether it's helping them get to the cloud or implementing a new financial HR system, we have to do it securely. And what we're seeing in the market is that it's really important to get right from the first time, whether it's a new application, a new network, a new platform, whatever, that if we can integrate security in earlier, it has better outcomes. And that's one of the reasons why we're hearing a lot of things about, things like DevSecOps these days. -Oh yeah, DevSecOps, so all of us viewers, and I know what that means because we had our Agile and DevOps TQ Aftershow. So, Ryan, that's when we think about embedding security right into the continuous development integration processes from the start, right? -Yeah, I think one of the biggest myths of security is that it's the party of no, that it stops progress, or it stops innovation. And what we found is that if we actually get security right, If we engineer it into the process, if we integrate it into those systems, we can actually get there faster and cheaper than doing it without. It doesn't always have to be a big bang approach either, like, we've invested a lot in our innovation and our intellectual property in tools and accelerators that can help our clients get there faster without spending a fortune. -Okay, yeah, and I do think that's a myth, and I'm actually glad you mentioned a myth because we've already learned a lot in the show, but we're going to take a break, and we're going to talk about myths in a few minutes, where we're going to really talk more in depth about things that people misunderstand about security. But before we get there, so I heard you mention accelerators. So Paulo, maybe you can expand a bit on that and give an example of what it means to us that don't know so much about this space, and what is an accelerator in the security world? -Yes, it's a pleasure. I think, that we need to keep it simple. So, an accelerator is something that makes an existing processor go faster, like a tool, like an asset, but let me share some great examples. The first one, about cloud, we talked about cloud. Cloud is a hot topic right down and the top priority, you know, for Accenture. And it is also a space where we have been able to innovate. So, we have developed an accelerator that can deploy specific security controls in a few hours, a task that used to take months. So, quality deployed in much, much less time. This accelerator recently made a huge impact in a cloud transformation in our bigger financial services client. Another great example is about application development. Think about application development, it's based on speed, but as teams embrace cloud, Agile, DevOps, security often is left a little bit behind because it can be too slow or inefficient. We have instead created an accelerator that integrates security into development life cycle without slowing it down to orchestrate the services that can help clients to find and remediate a critical issues at scale. In this way, we actually accelerate the development up to 30% in a large telco provider.

Myth or Reality?

-Okay, so we've already dispelled one myth that security doesn't slow us down, and there's plenty of ways that we can actually accelerate it. So, let's talk about a few other myths. And here on the TQ Aftershow, we always like to play games. So, we're going to do a rapid-fire session called myth or reality. I'm going to bring up a few things that I've heard about security, and you're going to tell me is it a myth or reality, and you have to tell me why in 30 seconds or less. -Just 30 seconds, Sarah? Ugh, I wish we had more time. -I know, but, you know, sometimes you only have 30 seconds in an elevator with a client, and I do have to say, I mean, not any of you, but sometimes at Accenture, we can be a bit verbose, so this is a chance to try and be really crisp with your messaging. Okay, here we go. Kelly, this first one's going to be for you. So, myth or reality? Security is only an IT department issue, 30 seconds, go. -The answer is myth, and let me explain in 30 seconds. So security is everybody's responsibility. Humans are usually the ones with the weakest link, if you will. And the buyer landscape is changing, we're not just talking about IT leads anymore, we're talking about everything of the company, from manufacturing, and even research and development, all the way through what happens to the end customer. So everyone is really responsible for security. -Great, and you did great on the timing, so I love it. And I do think it's a wonderful message, is that each of us have such a huge responsibility when it comes to security. So, Ryan, you're up next.

Myth or reality, it's possible for a company to keep the hackers out? 30 seconds on the clock starting now. -That is a myth. It is possible for our clients do everything they can to put in layer defenses because the threat landscape is constantly changing, new vulnerabilities are constantly being found and exploited, and so our clients to think about doing both, repelling the attackers and staying ahead of them, so that once they're inside, they can get them out. -Okay, okay, I like it. Good, good on the timing as well. Okay, Paolo, this one is sort of related, myth or reality, having security compliance, so you're compliant with all security means I'm secure as a business. -Well, it's a very large, big myth. So many of the most famous cyberattacks happen when the businesses were considered compliant with some regulation. So please think about Target, Yahoo, Maersk, also only some examples. Businesses need to be more than just compliant. Considering the threat landscape, they must implemented the right security countermeasures to protect themselves. -Yeah, it's a great, great reminder that you can't stop at compliance, so always staying vigilant, looking for vulnerabilities. There's a lot to do out there for sure. Okay, thank you, Paolo. Neha, your turn. Myth or reality, cloud is not secure? -Another myth. So actually almost 70% of cyber risk managers believe that digitization has made their organization more vulnerable to security compromises, but luckily, there are so many ways to make cloud secure. We mentioned some of our accelerators, we can block insecure configurations before they're even made, and we deliver them to our clients every day. -Yeah, that's great because I remember that was one of the key things we talked about on our cloud show, where clients were, you know, hesitant to go to the cloud because of security, so it's great to hear that. Okay, last one, back to you, Kelly because you are our global security lead, after all, I have to give you the most. So, myth or reality, hackers just go after those big companies? -Oh, huge, huge myth, and let me explain. Hackers go after the companies or the easiest way to go after what they're looking for. Sometimes it's the big companies, but many times it's the small companies also that actually, they use that as a path to get into the big companies. And so no one is immune to this risk. -Okay, great. -And Sarah, I have a bonus one. -Okay. -Don't all hackers wear dark hoodies? -Yeah, I think that's reality, right? it has to be. -Well, you know, that's what, we see them all the time in PowerPoint, or videos, or what have you, but I will tell you, I've been in this game for about 30 years, and I've never seen a hacker wear a hoodie, never, not once. So I think that's also myth. -Okay, good. So we will not use that as our detection for hackers, and it is interesting that, all in this game, all of the answers were myths, which I think just goes to show there's a lot of misunderstandings about security, and it's great that we're clearing them all up today. So thank you all for participating in the game. We do love to play games here in the Aftershow, and hopefully all of you, as learners out there, have figured out where these are myths and really set the record straight on security.

Key Takeaways

-So, we could continue to talk about security forever, but we do need to wrap it up, and as we've done on past shows of the Aftershow, we like to do one last round robin with all of you as our experts, and this time, maybe you can each just tell us what's one key take away you would have for our learners as it relates to security. So Neha, let's start with you. -I'd say that security does not equal slow. Our team is creating new solutions and accelerators to deploy solutions fast every day. So really, there's there's a lot that we can do to speed up the process and even make the whole transformation, whatever you're trying to do, actually faster. -Yeah, that's a great one. Thanks, NeHa. -Paolo, what about you? -Oh, let me highlight finally that security is everyone's responsibility. So it is ensured that not only by your security expert, but also by all the people in a company with the right behavior. So, in my opinion, security is not something that if you ignore, it will go away. So it's our job, but everyone's responsibility. -Yeah, definitely. It's not something we can each think that someone else is taking care of it. We each need to do that as well. Thanks, Paolo. -And Ryan. -I think, well, for me, I think it's about the fact that being secure is not just checking a box. You have to constantly and continuously review, work on it, improve, it's a continuous journey for us and our clients. You're never finished, you're only ever better. -Great. I love that point. Thank you. Okay, and certainly last, but not least, Kelly. -Alright, well, thank you. You know what, I'll tell you for me is I think that everyone needs to be a critical thinker. What, wow might it go wrong, so that whether you're deploying cloud or you're building a new supply chain for a client, we need to be critical thinkers about that. So it means all of us, you, everyone watching this video. So I believe that we have to take this to our clients, help them understand how to be safe throughout their whole enterprise, and every project on every program that we do. So I think that's, that's really our charge to everyone that's watching the video. -Yeah, definitely. Great take away. Well, I learned a lot about security today, and I want to thank all of you, Kelly, Neha,, Paolo, and Ryan. Thanks for spending your time with us, And I guess I would say thank you to our special guests, Bob and Brian, but don't forget, for all of us within Accenture, continue to strive for your gold IS Advocate badge. And I really hope that all of you now better understand what security really means and why it's so important to us and to our clients. And of course, you can always learn a lot more, so go to the Go Deeper section on our TQ home page. You can find links to great security materials and case studies. So keep learning, and we'll see you next time. This is Sarah Dugan signing off from our virtual TQ HQ. -Hey, how do you think they didn't Cash? -Pretty good, Brian, I mean pretty good, Tango. Yeah, I know I'm way more comfortable talking about security with my clients and of course, my grandma. -Of course, I agree, but wait a minute, hey, our transmission's being overridden. What's going on? -Get off my Aftershow.

Security In Review

What is Security?

What is security? Security is simply protecting against threats that would disrupt your normal way of doing things. Security is locking your door when you leave the house, keeping your money in a bank, memorizing your passwords. Businesses take many of the same precautions you do to protect their assets, data, and people. The tricky part is figuring out what makes a business secure. There are many facets to security. Controlling access to sensitive data so that a new hire doesn't have the same access as the CFO is part of a security plan, but so is making sure a warehouse has enough fire extinguishers in the facility. Our biggest focus is cybersecurity, protecting the data that is stored on devices like computers, mobile phones, and the internet. Losing control of information or a system can seriously damage a business's employees, its customers, and its brand. That's why we work tirelessly to avoid attacks and protect our digital assets. Bad actors will look to hack, steal, and disrupt personal financial and business information. It's not enough to simply react to security breaches when they happen. We need to be proactive to prevent them from happening in the first place. Security is sealing off vulnerabilities before they get breached.

What Does Security Do?

What does security do? It puts technical and procedural controls in place to reduce threats to your data, your digital identity, and your tech systems. These controls come in four different types and occur at different times along the threat curve. They are prevent, detect, respond, and recover. First, we put in controls to prevent anything bad from happening. The password you use to access your online bank account is a preventative control. We install controls that detect and alert us when something bad is happening, like how your antivirus software alerts you whenever it detects a virus or when you're about to go to a risky website. Then we use corrective controls that allow us to respond and recover from an attack. This includes things like incident response, forensic analysis to discover how they got in, and restoring the system using backed-up data. There are no absolutes in security, and it's impossible to prevent 100% of attacks because the threat landscape is always evolving. But you can and should do everything possible to stay ahead of the hackers.

Why Does Security Matter?

Why does security matter? Security matters because without it you may unknowingly overexpose valuable data. All systems have vulnerabilities and are susceptible to attacks. Some vulnerabilities are in the hardware, some are in the operating systems and applications, and sometimes the vulnerabilities are other people, like Sharon in Accounting. When one of those vulnerabilities gets exploited and an attack succeeds, it can damage your company's reputation, cost it huge amounts of money, and even shut it down temporarily. But it's important to look on the bright side and think about all the millions of unsuccessful attempts that are blocked every day. If your organization has the right types of security controls in place, you have a better chance to quickly find and fix those vulnerabilities and block the attacks. Security matters because it protects us. We can't be trusted advisors to our clients if we can't protect ourselves. It protects our clients. When our clients undergo transformations like moving to the cloud or adopting new services, they expose their organization and users to new risks. We owe it to them to protect their business at every level. It's expected. As the world gets more digital, people share more online and expect their data to be handled securely. And finally, it's the law. Governments around the world have recognized the importance of data security and are passing comprehensive laws like the EU's General Data Protection Regulation. Security matters because it allows businesses to keep running as usual, despite the never-ending threat of attack.

How Is Security Applied?

How is security applied? Comprehensively. Security should be at the center of everything a company does. It should be part of all their operations and every aspect of their business. Security is more than protecting your credit card number of securing online payments. It's ensuring a process is protected end to end. Let's look at how security is applied in a few common situations. Security breaches are especially dangerous when processes are interconnected across an ecosystem, like healthcare. Just think of how often your personal medical information is gathered and stored electronically: at the clinic, at the doctor's office, at the other doctor's office, at the hospital, at the pharmacy. It goes on and on. No matter if it is a single attack or a distributed one, a data breach or system interruption will impact the health care business, their providers, and their patients. That's why data theft, system disruption, and compliance with privacy laws keeps our health and public safety clients up at night. But you don't have to worry because the threats are mitigated by safeguards we put in place to make sure your personal data, insurance information, and healthcare information is all protected and secure. Applying data security protects your privacy, your payment information, and your treatment plan, so you can concentrate on getting well.

How Does Security Work?

How does security work? Security has many different facets, and they all need to come together in order to make it work. It's not just about tools and sophisticated applications and systems. It needs to start with people and processes. First, we identify an organization's tangible and intangible assets of value. This starts with a risk assessment, where we prioritize which parts of the business to focus on protecting. It's a critical first step in developing a secure organization. Next, we work to determine what needs to be done to protect the assets. We evaluate any existing security controls and find where there is room for improvement. Once the organization's vulnerabilities are known, we can determine the right controls, tools, and processes to protect the business. Then we manage and monitor those security controls on an ongoing basis. Keeping a business secure is not a one-and-done implementation. The threat landscape is ever changing. Hackers will always become more sophisticated. They will continually get better at predicting the patterns of existing security programs. Constant vigilance is the only way to detect and mitigate the ever-present threats.

What is Accenture's Role with Security?

What is Accenture's role in security? Accenture's security mission is to secure the world for our clients. We strive to be trusted security partners for our clients. We are the ones who can solve their most complex cyber challenges. Accenture Security partners with our clients in every aspect of security, including strategic and advisory services, system and architecture design and implementation, and full virtual and on-site management of entire security operations. The practice is built around three main services where Accenture can bring the most value to our clients, cyber defense, applied cybersecurity, and managed security. Cyber defense is how we assess where our clients are today, applied cybersecurity is how we build and transform our clients' security programs, and managed security is how we run their cybersecurity operations from our global delivery centers. Accenture is different from the rest because we have deep industry expertise, unparalleled strategic acumen, innovative ecosystems, and the global footprint needed to secure our clients' value chains from end to end.

How Does Security Combine With Other Technologies?

How does security combine with other technologies? Security is an important component to everything we do at Accenture. We want people to remember, whatever we are delivering, we must deliver it securely. Accenture Security needs to be part of the initial conversation and the eventual solution. Security should combine with all technologies, but let's take a quick look at some emerging technologies. Artificial intelligence, AI, provides opportunities to automate business processes and improve efficiency throughout the organization. However, it can also present new security risks. The good news is that the same AI technology that introduces new risk is also the same technology that can help detect and prevent risks. Using machine learning, ML, algorithms can help systems quickly identify threats that were missed by traditional security mechanisms. And then there is cloud. We help many clients migrate to the cloud, and as you might expect, it's important for us to do it safely. Sometimes security can feel like a roadblock that slows down the journey, but Accenture uses accelerators to help clients move to cloud faster than ever before. Blockchain, or distributed ledger technology, gives organizations a more trusted and secure way to exchange data. Blockchain innovations such as smart contracts, consensus, and on-chain data encryption, securely manage the access to and value of data. At Accenture, security combines with every technology.

TQ Security Wrap Up

TQ Security Wrap Up

Well, that's what we have for you on our core security content. I hope you've learned something new about security, and that you're feeling more confident and you can talk about it with your teams and clients, and even better yet, start to put these principles and mindsets to work for your area of the business. If you're looking for even more learning on security, visit the Go Deeper channel, where you can find specifically curated courses on security, and back to TQ home page, where we have our case stories and more. Make sure to tune in again soon for our next topic. Until then, keep growing your impact and growing your TQ. And happy learning.

Course author

Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched...

Course info

Level	Beginner
Rating	★★★★⯪ (385)
My rating	★★★★★
Duration	1h 27m
Updated	7 Oct 2020