MIT SMR CONNECTIONS

EXECUTIVE CONVERSATION

Cybersecurity: Keep It Basic. Keep It Collaborative. Keep It Strong.

COMMISSIONED BY:

DXC TECHNOLOGY

EXECUTIVE CONVERSATION

Mark Hughes,
President of Security,
DXC Technology

Boulton Fernando,
Vice President and
Chief Information
Security Officer,
Toyota Financial Services

It's no secret: Information security is a complex and ever-changing world fraught with risk. But adding the most recent tools to your organization's cybersecurity portfolio to try to mitigate new threats may be the wrong approach to security improvement. Today, it's more important to focus on taking care of the fundamentals, which are too often eclipsed by the latest market developments. Patch management, solid access controls, and good hygiene are often given short shrift in a cybersecurity environment that grows more complex by the day.

Getting back to basics means reducing complexity. It means keeping applications, databases, and operating systems up to date and disposing of old, unsupported ones. It means ensuring that you're getting the most from the tools you already have before investing heavily in new ones. It means establishing clear ownership and governance over data. Above all, it means doing the tireless work of promoting security awareness while also understanding that your people represent the front line of this defense.

In this Executive Conversation, we'll discuss what our organizations do to strike the right balance in all those areas. We'll also share our thoughts about the benefits of taking more inclusive approaches to building security teams and to collaboration as an essential component for success.

"Organizations can employ armies of security people. But by definition, the basics don't require security specialists. It's really about people using healthy practices. It also requires a tighter focus on governance so that the people in charge clearly understand their responsibilities."

SETTING THE STAGE

If you unpack the cybersecurity incidents that make the headlines, you'll find that very few of them are carried out by truly sophisticated criminals. Often, some of the biggest, highest-profile attacks are relatively simple in terms of how the threat actor managed to penetrate and compromise an organization.

It's a fair question: When we have all these security investments and tools, why are threat actors successful at getting into organizations and delivering malicious software through relatively simple means? To answer, let's start by looking back. The IT landscape used to be fairly self-contained, with a reliable perimeter supported by an element of trust. The job of cybersecurity was to protect that perimeter and everything inside it.

With digital transformation, that environment is much, much more dispersed, and that same level of trust doesn't necessarily exist. The move to cloud and applications delivered as services has exposed the troubling fact that security basics often hadn't been deployed as well as they should have been. In the past, you might have been able to get away with not having all the basics in place — maybe the firewall settings weren't right, or you didn't have the right identity and access control or patching regimes in those environments. That's no longer the case. Our dispersed, mobile, multi-cloud environments make it essential to have all those basics well covered.

Organizations can employ armies of security people. But by definition, the basics don't require security specialists. It's really about people using healthy practices. It also requires a tighter focus on governance so that the people in charge clearly understand their responsibilities.

At Toyota Financial Services (TFS), we're relying more heavily on biometrics as a basic element of access control. People are getting quite accustomed to using features such as Face ID, and we can use Windows Hello to log in, for example. But we need to have the industry move faster in this space because even when people are using Face ID, a password is still the underlying control. For instance, when you log back onto your iPhone for the first time after powering off, you don't get the option to log in with Face ID — you first get the password prompt. The industry is moving to put more weight on biometrics than on the PINs and passwords that are there now. But some of the legacy applications that can't use biometrics are holding us back. We need more development in that area, but it's difficult — if not impossible — to adapt the legacy systems for biometrics. In the meantime, we are using password managers to help our people resist the temptation to write them down on a yellow sticky note.

As part of the financial services arena, TFS is in a heavily regulated global industry. Our crown jewel is our customer information. Toyota customers rely on our quality, dependability, and reliability. Trust is a very important aspect. It's hard to earn trust and very easy to lose it. So beyond what the regulations require, we pay a lot of attention to protecting customer information. We rely on DXC to help us with that major undertaking.

MINIMIZING COMPLEXITY IN THE CYBERSECURITY LANDSCAPE

At TFS, one practice we've adopted over the past two years in information security is: If you bring in a new tool, throw out an existing one. For instance, if we're bringing a new endpoint detection or response system, do we really need that old antiviral solution in there?

Everything needs a reason to exist in the ecosystem. Given the human tendency to run toward the next shiny object, it's sometimes been a challenge to identify the right reasons. The TFS security team often wants to try new tools. We have to sit down and have that conversation together: "I understand you want to go get another tool, but can an existing tool suffice with a little bit of modification?" At TFS, we need to plan for tools with very long life spans because the United States is just one country we support. We also provide security as a service to 40-plus other countries globally with a lot of help from DXC.

We can't just adopt new tools in the blink of an eye. We need to look at the ramifications of what will happen when we change the tool worldwide. Does the new tool have language support? Are there local subject-matter experts out there who can help support the users?

The fact that we operate in 40-plus countries serves as a kind of protection for us against jumping from one tool to another. We aim to make full use of each tool and ensure that it has anywhere between a five- and seven-year life span within the Toyota ecosystem. Those are some of the countermeasures we have in place so that we aren't shopping for every new tool that comes out. Whenever someone asks to bring in a new one, we start a discussion with many different roles at the table. The product owners think it through and say, "What gets brought in here? How will it get used overseas where there is no support? Are you willing to provide the support?" The length of time it takes to evaluate a product slows down the influx of new tools. We are rather lucky to be in that position rather than automatically going after all the new options being marketed.

But many organizations do struggle with making the best use of the tools they already have in place. Generally, the industry is very keen on more and more tooling. At DXC, we often see customers who haven't yet fully implemented a particular tool, which falls out of favor before it's fully deployed. That means much of its value is never attained before a new tool appears. It's important to be very careful about swapping things out without considering what's already there and the utility you could realize if you just finished deploying it.

At DXC, we spoke to the head of security for a bank recently. He said they're running more than 40 separate security tools. That was incredible! Even running four or five tools is a complex undertaking. Forty-plus tools equal worlds of greater complexity. And in the age of mergers and acquisitions, a lot of complexity grows organically as organizations come together. The acquired organization often has a different set of tools that may not mix with the acquirer's security tools. There's a sort of "Venus and Mars"-type argument about which is right and which is wrong. Often, these things don't get resolved.

> **"For TFS, COVID-19 was a blessing in disguise for staffing. We went to a hybrid-work format that enabled us to tap into a community of people who are neurodivergent, who like to work on their own at home, and who have very good analytical skills."**

At DXC, our customers tell us they just want to reduce their internal enemy — complexity — and be more efficient in their approaches to security. The good news is: The market is beginning to listen, and we're seeing some emerging ecosystems that are trying to meet that need.

Many DXC customers believe they should reduce the complexity of their security environments to reduce costs. In reality, it's often more of an efficacy issue. It's simply inefficient and ineffective to have someone trying to toggle between five or six different screens simultaneously, trying to pick up what can be very weak signals from threat actors. But it's critical to be able to pick up those weak signals so that you can potentially avert a major problem. Having a high level of complexity in the environment makes that job a lot harder. Promoting simplicity should be a priority.

At TFS, as part of our efforts to simplify, we're encouraging people to be more accountable for their own information security. One initiative involves getting developers to be more and more responsible in this regard. We're training all of them in cybersecurity and secure application-coding techniques so that when they develop code, they can build in security — kind of a "you code it, you own it" approach. Historically, the developers would rely on security champions or coaches to do things such as check code quality from a security standpoint. Now we get the developers to do it themselves — that is, we're *going* to get them to do it. We're not quite there yet.

The overall strategy is to provide developers with the necessary tools and let them know that we're there if they need us. We have adopted a guideline that 20% of their coding time should be dedicated to compliance and security-related work. This includes patching, updating their products, making sure they're integrated with the identity and access management solution, and so on. We did this partly because we have a shortage of security personnel at TFS. We have about 110 teams that work on application development, and we just don't have that many security personnel to support all of them from start to finish at this point. So we had to empower them and step back a bit. Security tools are important, but this is about bringing in the community to make sure they do what's needed. Embedding security in the most relevant place for that work to be done helps reduce complexity and increase efficiency.

This is part of the industry's move toward DevSecOps, which expands the collaboration between development and operations to integrate security earlier in the software development life cycle. With digital transformation, speed is of the essence, but at the same time, risk shouldn't take a back seat. DevSecOps now helps information security move closer to the business more quickly, making business users part of the security solution. We don't want information security to cause lag time. The move toward DevSecOps, or "shift left," as the industry calls it, helps. It's made both our stakeholders — the business as well as IT — more responsible and accountable for information security. Are we there yet? At TFS, we're not. But we're on the journey.

> **"At DXC, our customers tell us they just want to reduce their internal enemy — complexity — and be more efficient in their approaches to security. The good news is: The market is beginning to listen, and we're seeing some emerging ecosystems that are trying to meet that need."**

TAKING A MORE INCLUSIVE APPROACH

As mentioned earlier, TFS is among many organizations experiencing a significant shortage of information security personnel. Some estimates indicate that more than 700,000 cybersecurity positions urgently need to be filled in the U.S. alone. Clearly, we have to leverage new hiring pools. For TFS, COVID-19 was a blessing in disguise for staffing. We went to a hybrid work format that enabled us to tap into a community of people who are neurodivergent, who like to work on their own at home, and who have very good analytical skills. We are partnering with organizations such as the National Organization on Disability to help us understand the unique needs of this community and work with them more effectively.

We have other initiatives to reach previously overlooked worker pools. For example, we're working with local universities to help grow future leaders in information security. We bring students on as interns during their sophomore or junior years. They work on projects that let them see whether they're a good fit to join our organization on a more permanent basis. From a Toyota perspective, we think very long term about employment. We do a lot of work with women-in-technology organizations, including an employee-led internal group called Women Influencing and Impacting Toyota. A significant portion of the TFS security team is made up of women. We also work with veterans, where we partner with several organizations, including NPower. It doesn't make sense to constrain our organization by not drawing from the entire pool of potentially available resources to help us fill our security roles.

As an organization, DXC highly values inclusion and diversity, so we look for ways to attract people earlier in their careers. We look for people who have aspirations of working in cybersecurity. We want to get to a place where parents add "cybersecurity expert" to the list of professions they'd love to see their children pursue. As a field, security is often viewed as very male-dominated and traditional in its practices. But if you think about it, security needs to be as modern as possible. Threat actors come up with new tactics all the time. You have to

stay extremely current. So with security, an extensive amount of experience isn't necessarily an advantage. Quite often, it's the opposite. Understanding the psyche of threat actors, how they operate today, and the best way to spot those types of weak signals often has nothing to do with how many years of security experience someone has.

At TFS, we've had good luck with bringing in people with different types of experience to join our information security group. Many strong candidates haven't had computer science backgrounds. Instead, they had degrees in areas you wouldn't expect, such as psychology or Greek mythology, and they've been very successful in information security. We've also had people who started as project managers and are now cybersecurity executives. In our field, you're always trying to think of all the ways things could go wrong. It pays to come at that problem from many different angles. We have seen that in action.

ESTABLISHING OWNERSHIP, GOVERNANCE, AND ACCOUNTABILITY

Historically at TFS, we let the business leads and their technology counterparts decide who owns data and the responsibility for its security. But then we discovered they were giving access authority to data much more freely than we liked. Now we've brought in risk management, a separate function here, to partner with us and tightly control access to data.

One difficult issue in terms of governance is the case of a product that contains consolidated elements, with different business units using the same application. The big question: Who's the true owner of that application? We haven't solved the problem yet. We are leaning more and more toward taking a user population standpoint, in which a department "owns" the users. That's one approach. But if the application is risk- or legal-related, we tend to carve it out and give the responsibility to our legal team.

At DXC, with many of our customers, we often see legacy systems that don't have clear ownership even from a technology standpoint, let alone a business ownership point of view. We generally draw the distinction that someone is responsible for making sure the system is operational and running. But the risk of a potential compromise of that particular system comes down to how it's used, who has access, and what type of data is running through it. So there has to be input here from people who have familiarity with the system from day to day. Often, the IT operational piece and the ownership of the people who use that particular application may be quite different. It's not easy to sort out.

COLLABORATING AS A WAY OF LIFE

Collaboration is fundamental to TFS. We have a principle called *genchi genbutsu*, which essentially means "go see for yourself the situation onsite." So we always like to have information security champions deployed to the business/technology teams, which we call "domains." We don't lock our domain security champions into one way of thinking or only collaborating with their own team members. We want them to go see for themselves, have conversations with others, and ask questions.

It's important to collaborate and have cybersecurity people embedded within the parts of the organization that are responsible for the actual running and processing of the data and the customer information in our systems. We want them to understand they're not on their own, and it's not just all put on them, but as an owner of a system that is processing information, you do have responsibilities that you have to discharge properly. Collaboration is critical, but you still need to be diligent about understanding who is responsible for what, and making that very clear.

Collaboration is also central to the relationship between TFS and DXC. We work together as one team. We have developed a culture of collaborating and working together with a lot of open communication. Bottom line: Security should never be about "us vs. them."

Mark Hughes is president of Security for DXC Technology. He is responsible for DXC's Security business, including cyberdefense, digital identity, secured infrastructure, and security risk management. He joined DXC from BT, a leading global telecommunications provider, where he most recently served as chief executive of BT Security. Previously, he held a variety of senior positions at BT, including key government customer-facing roles. In 2013, he headed the development of BT Security, which has become a global leader with 3,000 cybersecurity experts in 15 security operation centers worldwide and recording double-digit annual revenue growth.

Earlier in his career, he was the commercial director at MWB Business Exchange. He began his career in the British Army. He has served on national boards, including the Cyber Growth Partnership for the United Kingdom and the World Economic Forum's Global Cybersecurity Board.

He received a bachelor's degree with honors from the University of Leicester and trained at the Royal Military Academy Sandhurst and the Junior Division of Staff College. He received military advanced certificates in French and German from the University of Westminster.

Boulton Fernando is vice president and chief information security officer for Toyota Financial Services. He is responsible for safeguarding the technology infrastructure and data across the TFS group of companies. During his 11 years with Toyota, his team has transformed information security from being a U.S-centric program to a "security as a service" global offering. He is also accountable for developing and implementing best-in-class cybersecurity mitigation strategies, role-based access controls, context-sensitive data loss prevention programs, global security operation centers, and cybersecurity policies and standards, as well as developing and implementing forward-looking security road maps. He currently leads the effort to "shift information security left" as part of the TFS group's digital transformation journey, and he champions initiatives to grow new leaders and increase diversity in cybersecurity. He received a master's degree in information systems audit from California Polytechnic State University.

ABOUT DXC TECHNOLOGY

DXC Technology (NYSE: DXC) helps global companies run their mission-critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private, and hybrid clouds. The world's largest companies and public sector organizations trust DXC to deploy services to drive new levels of performance, competitiveness, and customer experience across their IT estates.

Learn more about how we deliver excellence for our customers and colleagues at DXC.com.

ABOUT TOYOTA FINANCIAL SERVICES

Toyota Financial Services (TFS) is the brand for finance and related products for Toyota in the United States, offering retail auto financing and leasing through Toyota Motor Credit Corporation (TMCC) and Toyota Lease Trust. TFS also offers vehicle and payment protection products through Toyota Motor Insurance Services (TMIS). The company services Lexus dealers and customers using the Lexus Financial Services brand. TFS is made up of affiliates in more than 40 countries. Wherever we operate, we aim to have a positive impact on the communities in which we operate. Our products and services differ from country to country to meet market conditions and regulatory requirements, but around the world, we are a company focused on delivering quality products that meet our customers' needs. Learn more at toyotafinancial.com.

COMMISSIONED BY:

DXC TECHNOLOGY

MIT SMR Connections develops content in collaboration with our sponsors. We operate independently of the *MIT Sloan Management Review* editorial group.