[Music Intro]

[Nataly] Welcome to Episode 2 of Shaping Global Markets. I'm your host Nataly Arber. If you're just tuning in, this is a series focused on key topics in the regulatory and financial technology space. Every episode, I'll be joined by industry experts, and we will try to answer some of the most asked questions. And we would truly love to hear from you about topics you want us to cover as well. So please, subscribe, leave a comment, or follow us on Twitter @DFINsolutions.

I'm truly excited to speak with today's guest. Not only is he the chief information security officer at DFIN, Dannie Combs is a self-proclaimed OG of cyber security and he has been working in the field for more than 20 years. In that time, he has held many positions across industries, and contributed to several publications as a leader in information security, including Corporate Secretary and Forbes. Notably, he served in the United States Air Force for eight years, managing information security and risk mitigation activities for the North American Aerospace Defense Command, Air Force Recruiting Command, Pacific Air Forces, and various intelligence agencies. Most recently, before joining DFIN as senior vice president and chief information security officer, he worked in telecommunication.

Welcome Dannie! I'm so excited to have you here today to talk to us in Chicago, on this brisk morning.

[Dannie] Thank you for having me.

[Nataly] Absolutely! So, before we dive into some of the bigger topics that we'll talk about that affect our industry, I wanted to take a step back and find out a little bit about your career trajectory, which ultimately led you to this senior position at DFIN. You have an impressive history beginning in the Air Force, where you earned two Air Force Commendation medals and five Air Force achievement medals. So, first, thank you for your service! But, also, I'd like you to just tell us a little bit about your experience in the military and how that influenced your interests in career.

[Dannie] Absolutely. First, thank you for the fantastic introduction there! So, I did spend eight years in the U.S. Air Force. I was very fortunate, primarily because of the era to which I joined. Back in 1993, technology was really just taking hold in corporate America, coming out of the basements of government facilities and universities, as did security. Secondly, relative to the opportunities that that provided, I'll give two examples.

I remember going to my first DEF CON conference in 1995, and DEF CON if you're not familiar, it's a very infamous hacker slash security researcher conference that's held every year in Las Vegas, Nevada. There were probably 150 people that attended that conference. It was fantastic because we would share outcomes of our research, we'd share tools and scripts, and things that we had developed. We would learn more about the latest trends of attack techniques and motivations, and, etc. Not to mention interact with, interestingly, your adversaries. Last year, or this past August I should say, there were 30,000 people that attended.

[Nataly] Wow!

[Dannie] I give that reference point because it's inspiring to me, just how rapid my professional domain has grown; how much has come to the forefront. I remember for many years, both in the military, as well as in the corporate context, my first office in the at Abbott Laboratories, a large pharmaceutical company, was in literally, in the basement of an IT building on their campus.

And today, I present quarterly to the board of directors of a billion-dollar company. Right, so, it's been quite the rapid trajectory, relative to the reliance upon security for organizations, the opportunities it provides for individuals such as myself. Going back to the Air Force, I just want to give a little shout out: my grandfather served on D-Day, and I was the third generation of men in my family to serve in the U.S. Air Force going back to the Army Air Corps days. My grandfather was one of the America's greatest generation that stormed Omaha Beach; my father, hand-carried the Panama Canal Treaty to the White House; I served in the era of the Kosovo-Yugoslavian conflicts, and Khobar Towers bombing, and 9/11 events. And I'm very happy to share my son is actually serving now, and interestingly enough, in the same unit that I did, for my final assignment, in the intelligence community.

To that end, when you serve in the intelligence community military, it really provides you fantastic opportunities, but they also have a unique budget structure. So, plenty of opportunities to work on advanced technologies, emerging technologies; you definitely get trial-by-fire, if you were fortunate to land those types of roles, and it really has served me quite well.

[Nataly] Can you talk about your experience seeing it evolve over the twenty years, and where you started in '93, to what it looks like now? It seems like it's more sophisticated, in different ways, if you could talk a little bit about that.

[Dannie] Sure. I remember reading the FBI annual security report in 2006, and there was a very important metric that just, just really blew my hair back; which was that cybercrime in 2006 had surpassed the global narcotics trade. And, for me that was definitely a watershed moment. When I think about the technologies that we employed, and the problem statements we were trying to tackle back in the late/mid 90s to the late 90s, they were a lot more simple.

Our biggest advantage, at that time, was just the knowledge of the underlying infrastructure and technologies of the operating systems. How the internet actually works, even as simple as how, when you type that email, there are six or seven steps that are actually transpiring in the background to route that message. Today, we take all that for granted. Today, it is significantly more sophisticated; we're less focused on firewalls, and major blocking and tackling. Today, as compared to even eight years ago, our approach was much more focused on infrastructure. Today, our approach is very much centered around data; today, the majority of the Internet is actually encrypted. It all appears to be the same protocols, as we'd say, of HTML traffic in HTTP, HTTPS, and so it's very difficult to identify those flows that will cause harm to an organization. And so, we have to employ different techniques. We've heard the buzzwords across almost every industry — artificial intelligence, machine learning — but where the security industry has truly embraced those capabilities and technologies, unfortunately so have our adversaries.

We've seen a number of AI-driven attacks; your "easier attacks" to mitigate are very often not the result of a human on the other side of that keyboard. Around 2010, I remember justifying my first large budget. I was meeting with the CFO and the chief operating officer (COO) of a 2.7-billion-dollar company. And, they were just beside themselves, that I was asking for 7.5 percent of the IT budget, which was interesting, because I had lowered it, to be in line with Gardner's recommendation of 7.5 percent. Right, and today, that's grown to be 14 percent.

[Nataly] Wow, so double in 10 years?

[Dannie] Correct, and that's not an insignificant number, obviously. Tens of millions of dollars are necessary. And that's to, again, tackle the well-known challenges that we all face. And that doesn't take into account the company-specific attacks that more and more organizations are forced to contend with from very sophisticated bad actors from nation-states, to criminal organizations in Eastern Europe, and in Asia. Where your standard controls just aren't going to be as effective.

[Nataly] With the complexities that have come, and adding more layers to keep things secure, it seems that sneaky tactics and phishing emails are still coming up as one of the primary sources for adverse actors, within a corporation. So, what if anything, maybe tactics or solutions, are there that we can keep top of mind to keep our data secure and keep the organizations in which we work secure?

[Dannie] It's a great question. It is surprising to so many when I share with them statistics around the effectiveness of phishing. While the sophisticated technology, that's brought to bear every day to compromised organizations is very effective, it is not as effective as a human factor has been of late. A large number of your large-scale breaches have been a direct result of simply crafting an email, and convincing the recipient to click on a link or to open an attachment. And that risk has been communicated for many many years. And so, it can be frustrating for a person, like me, to continue to struggle with this, if you would; however, there has been a more concerted effort. So, this year we've seen a surge in that type of malicious activity. And it's been interesting to see the bad actors specifically targeting named organization; doing the research to get to a named individual within accounting — it's very common actually — within roles like mine actually, because that can be quite embarrassing for a CISO to be compromised, but they, you know, the targeted campaigns have become very very common of late, very effective. Often the goal is to conduct some sort of financial fraud.

But it also serves as a fantastic delivery vehicle for a bad actor to gain access to a network or to a company by installing malware that's embedded into a word document or a PowerPoint or Adobe. Often, you'll hear us as security professionals speak of a dropper file, and all that means in plain English is you open up an Adobe whether a report and in the background is an application that's being installed. That is not malicious, but what that application actually does, is go out and download various malware and utilities that enables bad actors to gain access into your environment. So, it's often how ransomware is brought into an organization it's through a phishing email.

So, how do you prevent it? Certainly, there are technologies that are available, like PhishMe and Mimecast, and others, that provide both product and services to reduce the likelihood of a phishing event. But I think the most important tool is training. It is so vital that organizations commit to a security awareness training program that targets all employees, that further targets employees in higher risk roles with enhanced training, for example IT, security teams, finance and accounting in particular, the executive team. And, I also think that having an ongoing perpetual fishing exercise is extremely effective.

[Nataly] Shifting gears a little, although you've mentioned it a few times within our conversation already, but, in May of last year GDPR, the general data protection regulation, was put into effect and there have been offshoot regulations stateside as well, but it seems like many organizations are still struggling with the compliance with that regulation and the associated costs of it. So, from your perspective, what are some of the greater challenges that companies are facing?

[Dannie] So some of the greater challenges companies are facing would include just truly understanding what the expectations are. Also, being transparent in their analysis of what the risk is if they were to fall short, say if they were to have a material privacy breach event occur. What would qualify for a four percent penalty, four percent turnover that's in GDPR language, penalty versus a two percent turnover penalty. Mapping that back to their business activities — that's one challenge you know understanding the risk relative to the GDPR.

Second challenge is, there are organizations that, inappropriately so, they may not have had the same risk profile that warranted the same level of investment into security capabilities that a post-GDPR environment will require. And so, a challenge is, in that regard, would be education across the executive management team, to include the board of directors, but equally as important will be across the broader technology teams that have to design, implement and maintain those systems.

How they supported those systems will be different going forward in many cases. Example: what qualifies as an incident, from a security professionals point of view, has changed dramatically. Data may not have left the organization, but if it was mishandled by an inappropriate person internally, or a trusted supplier, you may have to disclose that. And even if it did — if data did leave your organization — but it wasn't a “hack,” it was a mishandling event, that may not have been reportable prior to GDPR, and it very well, slash, is likely, to be reportable today. So, how they go about their various work flows and their day-to-day activities, often needs to change, and their education across the employee community and supplier community needs to occur. And, those are pretty substantial challenges for a lot of companies.

[Nataly] Obviously, data protection is in the name, but do you think it's effective? Do you think that there is still room, where, because of the challenge and because of, maybe, how incomplete the prescription was when it was first given, that there's room to continue to be more in line with what the concept of GDPR originally was?

[Dannie] Yes and no. To your question — as it relates to are we seeing progress on their goals of reducing the overall volume of misuse and oftentimes flat-out abuse of privacy expectations — we are seeing it. We are seeing great progress. We are seeing one of those — an example that I appreciate as a practitioner would be that harmonization of expectations across each individual member state within the EU. That was so important to an organization, such as DFIN, as we're operating in the vast majority of them. Having a more simplified set of regulations if you would it's very helpful. I see that more in organizations that have embraced their expectations, and so, along with that comes more controls and overall respect for privacy. And a key tenet to privacy is security. So, they’re definitely having a very positive impact, here, domestically, in the United States – California, Tennessee, Nevada – their state laws have gotten a lot more teeth, and acknowledgement, quite candidly, their applicability, as a result of the sheer press the GDPR has received.

Where I look forward to some continued clarity would be, for example, what constitutes a reportable event? How are we measuring what is a material? I'll use the word breach, in a privacy context at least. What qualifies as a breach? We need more clarity there. What the penalty structure will look like? We need a lot more clarity there. And, as time marches on, we will continue to see more, but we're beginning to see through the outcomes of court rulings, just directionally, what to expect. We're getting more clarity, and I think that’s going to be very helpful.

[Nataly] I read in an article recently, that by the end of next year in 2020, 67% of enterprise infrastructures will be cloud-based, and 82% of the workload will reside on the cloud which doesn't seem super surprising to me, and probably most people wouldn't think that's surprising, but it does seem that there needs to be a much bigger focus on how do we keep something that is still a little bit elusive — that cloud concept — how do we keep it secure? So, from a customer perspective what should they look for when looking for a secure cloud solution?

[Dannie] Sure. So, there's two tracks of interest that customers usually want to focus upon. And within each track, there's three swim lanes of validation, so let me try to tackle, *all that*. First would be with your general security technology. It's so very important for organizations — that provide services, that produce products — to acknowledge that as they transform their portfolios to be cloud-centric, they must acknowledge that the technologies used in a cloud will be different from a security point-of-view; you need different security technologies for the cloud than you would for on-premise, at least for many of these use-cases we need to solve for.

Second would be, the processes that are in place. So, here at DFIN, for example, we illustrate the effectiveness of our security technology, the disciplined approach to process that we use to support the security technology, as well as the overall infrastructure and application solutions that comprise Venue and FundSuiteArc and other products that we offer, by way of instruments like the AT101 frameworks SOC 2 certification. In order to achieve that, we leverage global frameworks that provide a general guideline, and playbooks, to success for security. For example, the NIST, ISO 27001, and others. And so, we've selected the controls, and control activities, that are relevant for our business, and for our products, and relevant to our customers. And [we] created a defense cybersecurity framework that serves as our guiding principles to how we build and deploy technologies, how we monitor those technologies, both from an operational and from a security perspective.

[Nataly] From a customer's perspective, how external is that promotion of having those certifications? If those are cornerstones for a secure solution, how from an external point of view do you know that those are in place, and that it’s a priority for the organization that you're doing business with?

[Dannie] So a couple of thoughts. We pull the relevant components of ISO 27001, incorporating those controls and those expectations into our AT101 SOC 2 framework, as we'd say. And we hire a third party to perform a series of audits, and they attest by way of certification — when they issue the SOC 2 report — how well we are performing to those control expectations. We elect to presently use Deloitte, one of the best in breed organizations for assurance, and they're going to provide a true and accurate representation of how well we performed in this regard. We share that report, upon request from clients. We issue this report annually. Each of our products are in scope, particularly products like Venue and FundSuiteArc.

The clients certainly expect, that we not only provide evidence that our operational processes and the overall ecosystem that comprises these solutions is operationally sound, it's going to be available 24 by 7 [and] not be challenged with outages in the alike, unnecessarily. But they're equally as critical of the security of them, particularly the types of data that is entrusted to us within our Venue offerings. We also represent very mature security controls and privacy controls as part of that that same SOC 2 certification.

[Nataly] Okay, great! I think that's probably helpful for somebody looking for a cloud solution as they compare, and try to figure out what's best for them; so, thank you for that insight.

So, from a bit of a more personal, but also professional standpoint, who do you think is doing it right within the field? Who are you watching, companies, or leaders or people that have voices, that any customer might want to listen in on? But especially from your professional perspective, [who is] really changing the way we're talking about security?

[Dannie] So, I'll start with a couple of examples, and I'll try to think, because I think it's very timely given the evolution of cloud…from a cloud technology perspective, I talked today, quite a bit, about how strategies and overall approaches are securing those efforts.

The fine folks at Fishtech have really demonstrated a fantastic capability in a very short period of time. I believe, they've been in the market about three years now. But, they're rapidly demonstrating, they are a thought leader in cloud security from an advisory and overall services perspective. Probably because the founder and CEO, Gary Fish, being a bit of a legend in security industry. He started, matured, and sold several security products and services businesses to the tune of his last firm that was sold for, or is now valued I should say, at over two billion dollars. Which is the largest security services firm in the United States. So, he certainly has had a very successful track record.

Another example of services, because as it becomes so very important to have the right skill sets and the right roles when it comes to security. There's an also very successful organization named ReliaQuest, who's headquartered in Tampa, Florida. Their founder, and CEO, Brian Murphy, has done a tremendous job. When I met Brian Murphy and the team, probably 2011, I was so very impressed with a 35-40-person start-up organization, who was able to demonstrate such deep expertise around security operations, investigations in the moments that matter of incident response, and overall security monitoring. They are now 500-600 people strong, valued over a billion dollars, and they have some the largest brands in the world now entrusting *them* to be the frontline defense of monitoring for cybersecurity attacks and [being] the frontline response to mitigate those risks. So, that would be a second example.

The last example I'll use, would be, actually, that of Google. Who can be very controversial in the topics of privacy, depending on what we would like to talk about. But they have taken their successes, of the Google search capability, and extended that to enable security organizations to more rapidly obtain the insights across a very large and very diverse data lake, for example. So, imagine being able to go to a web browser — their product is known as Chronicle and it came to market in 2019. It is getting a lot of press, for possibly being the most disruptive security tool, in the last several years, because of the sheer speed to which we can query terabytes, upon terabytes, of data and get rapid responses. As the cloud, and overall internet, continues to experience explosive growth, you know one consequence of that is the volume of data that we have to monitor. And so, when you're trying to aggregate terabytes of information daily — sometimes hourly, depending on the organization — and you have to correlate 100's of terabytes, or a petabyte, of log data to find that needle in a haystack. They can take hours, sometimes days, to get the responses you're looking for. With Chronicle's capabilities they've really got that down to remarkably a low, period of time; just a few minutes

[Nataly] Wow, that sounds very interesting, and I hadn't heard of Gary Fish, so we'll take some reading back with us. One last question, just to bring this conversation sort of back to your personal habits. What is an application on your phone that you would recommend, that you feel helps you do more with your day or [helps] at work.

[Dannie] There are two. First would be OpenVPN. Most employees in 2019 know that if they're going to connect to the company's digital assets, they need to do so in a protected manner. So, the common practice is to connect over a company VPN. Why would you not protect your personal information? Such as all your passwords that can be extracted, or your credit card transactions when you're booking airline reservations, and the alike. I personally use VPN 24-hours a day on every device that I can. Which is almost all of them.

Secondly would be, I've acknowledged a long time ago that my information has been compromised, and someone's probably trying to compromise it right now. It's just that the world we live in today. And so, Google Authenticator — that multi-factor, two-factor application from Google, that is so widely integrated in Apple and Android markets; a very high percentage of applications have Google Authenticator integration, so that provides a secondary level of protection for me. In the event that my past has been compromised. Often times, at no fault of my own, because of bad apps and various vulnerabilities, and the like, you know, at least I had that second factor to better protect myself and my family.

[Nataly] Out of curiosity, do you think that the two-step verification, because I use that as well — it texts you the code and then you use that code to get into whichever application you're trying to — is that more secure, or maybe it's on par with, having your thumbprint, or using a digit as your secure password? [In other words] is having an imprint from one of your fingers more secure, or is it sort of two halves of one?

[Dannie] That is a fantastic question, for which we can have a five hours period. [*audible laughter*] One side of that coin says, your fingerprint never changes. So, if I were able to lift your fingerprint, for which it happens, you see in all the spy movies. If your fingerprint, digital or physical imprint, were to be compromised, then it's a one-time password, if you would. Whereas the, Google Authenticator, and other multi-factor solutions out there, issue one-time passwords that change within three minutes, or 30 seconds, depending on the platform. So, even if you were to compromise my 10-digit PIN from Google Authenticator, or any other application, you have a much more narrow window time to leverage that. My opinion…

[Nataly] Two-authenticator it is!

[Dannie] Yes, it is less secure to use your fingerprint. And then there's an entire rabbit hole we can go down about, “Where does that fingerprint go?”

[Nataly] Oh, that is a fascinating question. That does sound like a rabbit hole that we would spend a long-time in. So, thank you so much for taking the time to speak with us. I think that you gave some amazing clarity into GDPR, some of the other cyber things that people are concerned about these days, and how the future of that industry is being shaped and evolving. So, thank you for your time.

[Dannie] I appreciate the opportunity. Thank you!

[Music outro]