digicert®

# POST-TRANSFORMATION: BUILDING A CULTURE OF SECURITY

## Dean Coclin of DigiCert on How Banking Institutions Can Future-Proof Security

ISMG
INFORMATION SECURITY
MEDIA GROUP

digicert®

In the post-digital transformation world - and in advance of the coming of quantum computing - it's time to future-proof cybersecurity by nurturing a culture of security. **Dean Coclin** of DigiCert discusses how banking institutions can embrace this change.

In this video interview with Information Security Media Group, Coclin discusses:

- How to prioritize risk mitigation;
- Balancing security with customer experience;
- Preparing for the post-quantum world.

## WHY WE NEED A CULTURE OF SECURITY

**TOM FIELD:** Why is it more important than ever in today's digitally transformed institution to build a culture of security?

**DEAN COCLIN:** There are a lot of threats out there, and you have to live and breathe security every day because these threats are constant and they're not going away. Every day, we see threat actors trying to infiltrate financial institutions because they're looking for the dollars that they can reap from those potential attacks. Making sure that employees and their customers have a culture of security embedded in them has to be taught, and it takes time to do that. People have to be prepared because the attackers are getting much more sophisticated. They are using artificial intelligence to mimic employees of banks or customers and their families. This makes it important to have a culture of security embedded for employees and customers.

### DEAN COCLIN

Coclin has more than 30 years of business development and product management experience in software, security and telecommunications.

> "People have to be prepared because the attackers are getting much more sophisticated. They are using artificial intelligence to mimic employees of banks or customers and their families. This makes it important to have a culture of security embedded for employees and customers."

## MITIGATING RISK

**FIELD:** What are the most important risks to mitigate, and how can we do that?

**COCLIN:** There are a lot of different risks for financial institutions around outages. Having downtime on their websites makes customers very upset and if it is a constant occurrence, people are going to lose trust and move to another institution. So, it's important to have digital certificates, which secure those websites, up and running, not expired. If they're expired, then customers can't get to those websites. Make sure that you have valid certificates on the websites, encrypting the data between your computer and the bank server, and make sure you're at the authentic website that the bank is operating. These are key considerations for trust going forward.

Another thing that is extremely concerning to banks is phishing attacks. Everyone has seen these types of emails coming into their inbox. Many of them are easy to spot, but they're getting much more sophisticated. Being able to find a phishing email and discard it and not open it is very important. If you are phished by someone that pretends to be your bank, then your account can be withdrawn and the bank will lose money. They'll probably pay you back, but that affects their balance sheet, so they want to minimize phishing attacks as well.

Knowing your customer is also very important. Banks need to make sure they're doing business with legitimate users and not criminals, especially when people are doing things remotely. All of the technologies for knowing who you're dealing with are very important to financial institutions.

## SECURITY AND CUSTOMER EXPERIENCE

**FIELD:** Financial institutions need to balance security and the customer experience. How does one achieve this delicate balance, and what's at risk if one doesn't?

**COCLIN:** These are trade-offs that financial institutions make every day. How much security do we impose on our customers? If we impose too much, it's going to make it unworkable for the customers. They will get frustrated and do their business somewhere else. But at the same time, we need to make sure that the customer is really the customer and not some fraudster. There has to be a delicate balance between those two things. Most financial institutions have incorporated

two-factor authentication. And many times, at the beginning of the week or the month or if you're on the same computer, they do fingerprinting on the device that you're accessing the institution from as well as your location.

If normally you access a financial institution from New York City and suddenly you're in Singapore, that's going to raise a flag and prompt you for two-factor authentication, which has many forms. It could be in the form of an SMS message to your phone, but that is being discouraged these days because fraudsters have found ways to take over your cellphone and reroute those messages. Another type of authentication is digital certificates, which can be used to authenticate your account to the financial institution. Balancing security and the customer experience correctly is tough, but many financial institutions have figured it out and are improving it every day.

## FUTURE-PROOFING SECURITY

**FIELD:** How do we future-proof security and prepare for the post-quantum world?

**COCLIN:** Quantum computers are becoming more and more real every day – and not only in large companies like Google and IBM. Nation-states like China and others are building quantum computers with larger and larger numbers of qubits. If a quantum computer is constructed with a sufficient number of qubits, it could break the encryption that is used on the web today, which is RSA, and that would cause havoc for many types of businesses and industries that rely on that encryption to keep data private.

So, institutions are now playing around with post-quantum cryptography. These are different types of algorithms than RSA, and they are safe from quantum computers. The National Institute of Standards and Technology has an evaluation that looks at different types of quantum-safe algorithms. They're going to be announcing the winners of this competition shortly. It's not too early to start playing around with the different types of quantum-safe algorithms so that you will be future-proof when quantum computers come about, which is probably not going to be in the next few years, but maybe in five, 10 or 15 years.

## SECURITY CULTURE STARTS AT THE TOP

**FIELD:** How does a culture of security address the issues we've discussed, and what's at risk for institutions that fail to do so?

**COCLIN:** You really have to drive it home. Otherwise, it is not going to be pervasive in the organization. Training around cybersecurity and cyber incidents is extremely important, including regular training on spotting phishing emails, making sure that we're dealing with the people we're supposed to be dealing with and looking at the new technologies around artificial intelligence and how they have been used to circumvent security controls. The culture of security is extremely important for not just the people that are talking to customers every day but for everybody in the company, and it starts at the top. From the CEO down, the culture of security has to be broadcast to the workforce so that they know how important it is to protect the organization from ongoing cyberthreats.

> "It starts at the top. From the CEO down, the culture of security has to be broadcast to the workforce so that they know how important it is to protect the organization from ongoing cyberthreats."

## THE DIGICERT APPROACH

**FIELD:** How does a culture of security address the issues we've discussed, and what's at risk for institutions that fail to do so?

**COCLIN:** DigiCert is the authority on digital trust. We've spent over the last 20 years securing web transactions, code, email and anything you can think of that needs to have encryption and authentication. Verisign started this in 1995. It was sold to Symantec in 2010 and in 2017, DigiCert acquired that business. So, we have a long heritage of security in our background.

Some of the threats I talked about can be addressed with products that DigiCert offers. For example, anti-phishing can be addressed with a product called a Verified Mark Certificate. With this type of certificate, all your emails will show a blue check mark and a little hover card that says that you are who you say you are when a recipient opens that email in Gmail and Apple Mail. We also have a post-quantum cryptography toolkit for organizations that want to experiment with post-quantum cryptography now and not wait until the winners of the NIST competition are announced.

Many institutions are faced with ransomware. It is a big problem, and the government has focused on a software bill of materials. They're enforcing this for all government contractors, and it is now spreading to other verticals. A software bill of materials shows that the software you're getting is what it's supposed to be and has not been tampered with. Many banks and financial institutions deploy mobile or desktop applications that they build either from scratch or from third-party products. It's important to sign that code as it goes through the development life cycle, create a software bill of materials and ensure the integrity of all that before the code gets to the end customer. If the code was not signed during the development process, it can be injected with malware. That's another area where we can help organizations.

The biggest area where we can help is around certificate life cycle management with our product Trust Lifecycle Manager or TLM. Many organizations have no idea how many digital certificates are in their environment, probably because they're multinational organizations that acquire companies along their life cycle, and certificates are purchased from different vendors. When we do a discovery of all their certificates, they say they never knew they had so many different vendors and certificates out there. As certificate lifetimes start to shorten, it's very important that organizations don't let those certificates expire, which would lead to a loss of trust when you can't get to that website. TLM helps in that environment.

## About ISMG

Information Security Media Group (ISMG) is the world's largest media organisation devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io