IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

In Conversation

In Conversation with Michael Downs

Carol Baker

As the growth of MFA bombing continues to expose organizations, we talk to Michael Downs, Global Vice President Sales, SecurEnvoy about how businesses can identify, monitor, and protect sensitive information across their environment.

Founded in 2003 and supporting customers across multiple sectors in 36 countries, SecurEnvoy is a UK-based cyber security company specializing in access management, multi-factor authentication (MFA), and data discovery.

Michael Downs
Global Vice President Sales
SecurEnvoy
https://securenvoy.com/

Michael is a seasoned sales leader with over 30 years' experience driving growth in cyber security sales, specializing multi-factor authentication (MFA), data discovery and access management. As Vice President of Global Sales at SecurEnvoy, Michael works with organizations across the UK and internationally to strengthen defences against credential theft, phishing, and unauthorized access.

He leads the global sales strategy including channel partnerships, with a deep understanding of the UK cyber security landscape. He collaborates closely with VARs, systems integrators, MSPs, and distributors to bring scalable access management to help customers protect sensitive data, maintain trust, and ensure compliance.

Tell our readers a little about yourself.

I've got 30 years of IT experience working with channel partners globally, predominantly on the sales side of things, but across product as well. For the last 25 years, it has been purely in cybersecurity, selling to and through organizations again globally, and that's in enterprises and in telco.

SecurEnvoy is a British born, bred and based organization. We're a cybersecurity company that provides access control solutions, primarily multi-factor authentication, access management, and data discovery for compliance.

We have been established for over 22 years, developing security products and supporting customers across the globe. We are involved in multiple verticals, and have received two Queens awards, one for innovation and one for export. We are extremely proud of our achievements.

What range of multi-factor authentication (MFA) options does SecurEnvoy provide, and how do they support both on-premise and cloud-based deployments?

For us, the key thing is the customer experience. It's important to be as flexible as possible with the offering and the environment, providing solutions that support the user using software tokens, phones, any mobile devices, hardware tokens, key fobs, cards etc. We also have integration capabilities with the FIDO Standard, whether this be FIDO Compliant Hardware Keys or Software based passkeys, that enable phishing based authentication. We also operate with air gapped systems, and when you start looking into more defence related organizations, that's a very key factor.

SecurEnvoy also has the ability to provide for Managed Service Providers (MSPs) so that they can go and deploy it and take it as their own service as well.

In what ways does SecurEnvoy's adaptive Multi-Factor Authentication (MFA) and Conditional Access Policy Engine balance security requirements with user experience, and how does it adjust authentication levels dynamically based on risk factors like location and device reputation?

It's around that user experience – that's the important bit – and we've got a couple of ways of doing it. There's the different authentication methods, but we also have offerings around anomaly detection, such as identifying unusual behaviour, a change from the normal location that someone logs in from, etc.

How do SecurEnvoy's solutions integrate with existing IT infrastructure, such as Active Directory, to simplify deployment and management?

This goes hand-in-hand with the user experience. It's also how flexible can you deploy and how easy is it to deploy.

We've got flexible integrations that integrate with existing directories such as Microsoft Active Directory or Lightweight Directory Access Protocol (LDAP) directory, and cloud directories via API, such as Microsoft Entra or Google Directory. So, we develop the product to be as flexible and as easy to deploy as possible.

But what we also do is use some of the modern authentication standards, such as Security Assertion Markup Language (SAML2), and also the more long-standing authentication protocols, such as Radius, both of which integrate really easily into the applications that the customers tend to use nowadays.

The other thing that we have, and is a key differentiator for us, is that we allow our users to do bulk user enrolment. That means they can get a large number of customers easily up and running and using the MFA as quickly as possible.

Beyond MFA, what other cybersecurity capabilities do SecurEnvoy's solutions offer as part of a Zero Trust access strategy?

We have a number of offerings: Anomaly detection, as I say, so it will learn the way that you normally log on, what device, what time of day, what location, etc. and it will then assign a risk score to that. We also have something called 'impossible travel detection'. For instance, we identify your location when you log in (for example, UK), and then maybe ten minutes later you log in from a different location (for example, Canada) then that's a red flag.

We also have the ability to provide secure remote access via Virtual Private Networks (VPNs) and firewalls using Radius. Plus, we also have such things as single sign on (SSO), session management, and we have the ability to protect desktops and servers at login screen – that is a compliance requirement for some standards.

How do you explain to a CEO how Phishing-resistant MFA works?

There are two ways you can talk about the impact, but I think what's important to remember is that 80% of data breaches are down to weak passwords. So, if you can do something that will actually remove that, for instance, MFA, you are reducing that attack vector considerably.

Phishing resistant MFA will stop common attacks such as MFA bombing, and also allows you to protect certain critical systems as well – even if an employee makes a mistake.

Ultimately, implementing MFA as a best practice will reduce potential downtime and financial losses, as well as bolstering brand trust. It is also very simple to use and deploy. Not only is it a benefit to the business as standard, but it also comes in line with some of the global security agencies guidance .

When it comes to adopting new authentication methods, what is the impact on employee productivity and user experience, and what strategies (for example, training programs, phased rollouts) are effective in managing user resistance and ensuring a smooth transition?

It's all about that user experience. We invested a lot of time in development and listening to our customers, working with them, seeing what they need, and making sure that the experience is as efficient as it possibly could be for the company as well as the user.

We also offer passwordless solutions, eliminating the need to remember passwords. It should be very efficient and straightforward, and this is what FIDO2 allows you to actually do, which helps make our product line so successful.

How does the adoption of phishing-resistant MFA help the business meet current and emerging regulatory requirements and industry standards (such

as NIST or GDPR mandates) for strong authentication, and what are the potential consequences of non-compliance?

It's important to look at the potential consequences of non-compliance as well. There are a large number of national and international regulations and legislations which mandate MFA. For example: NIST, and if you look at their page, they make it very, very clear. It's very simple – what they say is, turn on MFA today.

Consumers also want it. Nine of ten (89%) say that using multi-factor authentication makes it feel that their online information is more secure, enhancing trust and reputation by offering it

In terms of costs to the business, there's regulatory fines such as GDPR, but then there's also things like ransomware and its impact on the business, not just operationally, but also the loss of business, and the impact on people people who work in that business.

What are the most common and effective techniques attackers use to bypass multi-factor authentication (MFA), such as social engineering, session hijacking, and MFA fatigue, and how do these methods exploit human or technical vulnerabilities?

The big one recently is being MFA fatigue or push fatigue. It is also called MFA bombing, which is where the hackers send multiple requests for MFA approval to users – and then, ultimately over a period of time, the user just goes, "right, I want to get rid of this", just clicks on "OK" and the system is compromised. That technique has been used for a number of high profile attacks. Phishing Resistant MFA will stop this. FIDO tokens will only initiate a challenge request to the device which holds the key to sign this challenge with, providing they are within close proximity to one another (using NFC and Bluetooth). If a threat actor is trying to impersonate a login from the legitimate user, they won't be able to initiate the challenge request as they are nowhere near the user.

Help desks also get fatigued from requests coming in. So, it is important that you have additional services on top, such as our help desk verification where the IT help desk can verify users using a one-time password sent to a device that's registered. We double check to make sure it is the user who is actually making the request, and we add to this our anomaly detection and impossible travel functionality. Today, it is important to deploy a combination of things to counteract MFA bombing attacks.

Beyond immediate financial losses, what are the primary business impacts of a successful MFA bypass, particularly concerning long-term reputational damage, legal liabilities, regulatory fines, and business interruptions?

This comes under a big banner of – and again I mentioned it earlier – trust.

If you think about when you have been let down in business and/or personally by somebody or some organization – the trust goes and it's hard to get that trust back. That relationship between the user and the brand is what we're protecting.

You’ve got to look at employee wellbeing as well. These attacks have an impact, and it’s not just a financial impact. There’s an impact on people – they begin questioning themselves “Was this me?” “Was it my fault?” You know, there’s lots of emotional aspects that need to be accounted for, and it’s important that the well-being of employees is protected.

If we look at it from a business perspective, it comes down to shareholder value. Typically, when a breach goes public, an organization loses about 7% of their market cap. So there’s a big shareholder value responsibility. But I think there’s also a personal side of it as well around the trust that an organization puts in employee well-being.

What are the immediate operational and financial consequences of an attacker gaining unauthorized access to internal systems via an MFA bombing attack?

By using the principle of least privilege, you can assign conditional access policies so that users only get access to the areas of the network or the parts of the business that they need. You also need flexible authentication methods. It is important to be stringent on those conditional access policies. A vanilla approach does not work. You need to really get into the detail of it and make sure that the access policies are correct for each – again, anomaly detection, detecting those weird logins from weird locations at weird times. If it is abnormal, you need to have the ability to log that request and notify administrators of any anomaly logins so that they can look into it. Having that inside the platform is a really, really key differentiator.

How do data breaches resulting from MFA bombing attacks affect a company’s long-term reputation, customer trust, and legal compliance obligations?

The bottom line with unapproved tools is they will have a lack of security controls. So if you are using any sort of mobile device, you have got to be able to manage those devices – and we can help with that with our data discovery tool that allows you to detect and remediate any sensitive data that you’ve got in the estate. If there is sensitive or confidential data on there that shouldn’t be, then we have the ability to protect the data, and make sure that access is done correctly.

With the increasing global demand for MFA continuing, how will SecurEnvoy expand its market reach and help organizations navigate complex information, data privacy regulations and access management worldwide?

We are very, very focused on what we do, and we are very good at the work we do. We have been doing it for over 20 years, and we have lots of happy customers. We continue to focus on giving our customers the best solutions, a lot of which are driven by customer demand.

We are also very flexible when we work with our partners. We’ve got a very strong global channel base, and work with industry bodies as well.

We continue to drive our innovation, but more importantly, make the best products we can in the market.

Any closing thoughts?

I think ransomware will become more prolific and sophisticated. You're already seen ransomware as a service evolve, so I think that will only continue. Organizations need to go back to the basics – they need to be able to secure their users and their assets as fast and as efficiently as possible. That's really going to be important. As I said before, 80% of breaches are down to weak passwords. So remove that weak link, put in MFA to get over that – MFA is one of the best and quickest security investments you can make to protect your business and your customers the modern day threats that we see today.