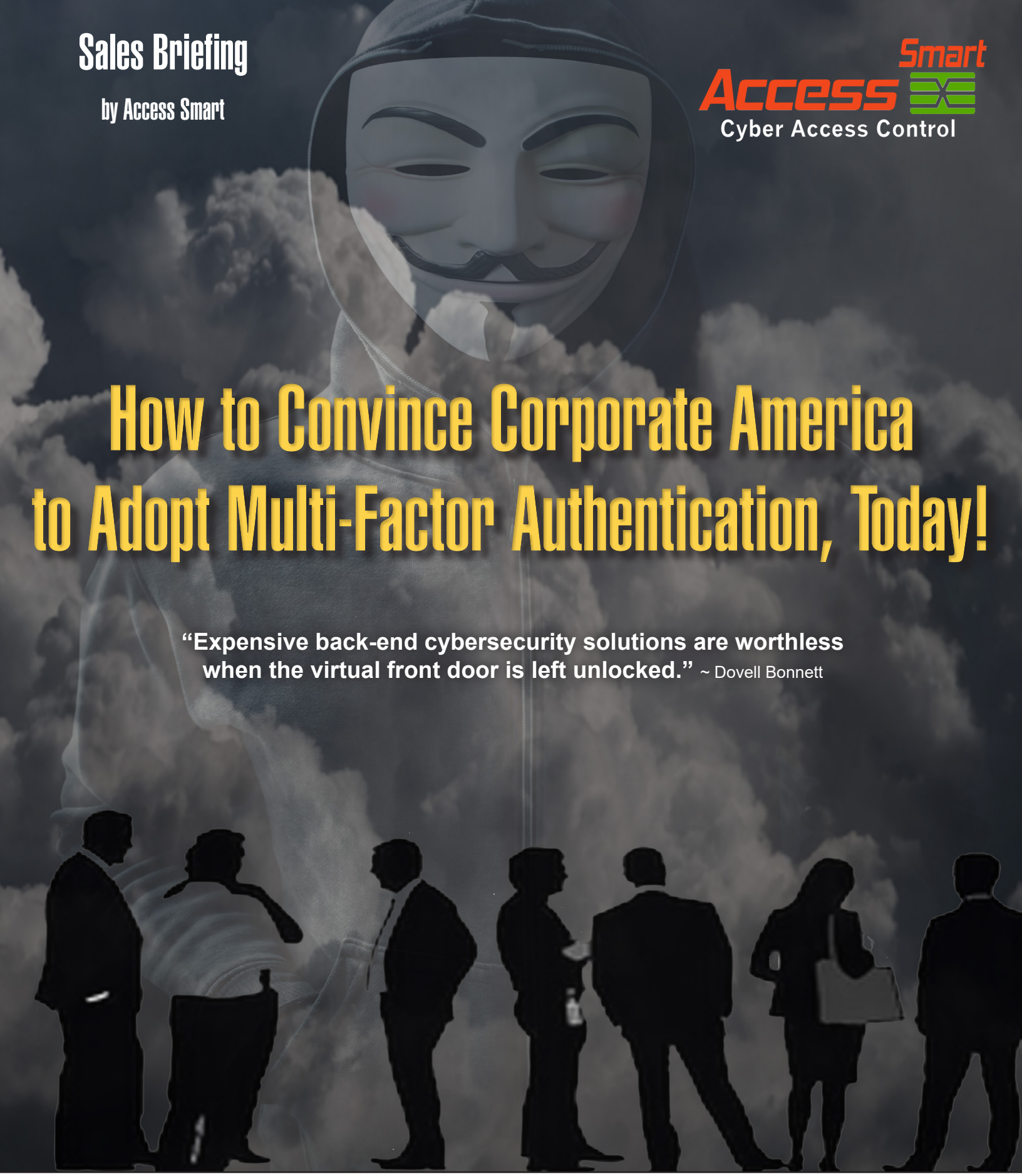
Sales Briefing

by Access Smart

Smart Access

Cyber Access Control



How to Convince Corporate America to Adopt Multi-Factor Authentication, Today!

"Expensive back-end cybersecurity solutions are worthless when the virtual front door is left unlocked." ~ Dovell Bonnett

Dovell Bonnett
Founder and CEO of Access Smart®, LLC

How to Convince Corporate America to Adopt Multi-Factor Authentication, Today!

By Dovell Bonnett, Founder and CEO of Access Smart. LLC

Cybersecurity reports and white papers post survey statics that scream for the immediate implementation of Multi-Factor Authentication (MFA). The statistics are eye-popping and the arguments for MFA are well thought out and compelling. So, why are companies still slow to implement MFA?

Most cybersecurity companies use Fear, Uncertainty and Doubt (FUD) to make their argument. The CIO needs FUD to understand their network's risks. The CEO, on the other hand, already lives in a constant state of FUD. Sales, revenue, customer satisfaction, new products, the board of directors, competitors, investors, and employee issues are just a few things weighing on every CEO's mind. Adding one more fear to their list isn't going to sway a CEO.

Two Silos

When selling cybersecurity products and solutions, there are two decision silos you must deal with: Technical and Financial. The technical silo consists of the CIO, CTO, and the CISO. The CEO and CFO make up the financial silo. Both have a vital role, and they look at the same problem from two totally different perspectives. That's why a cybersecurity salesperson must have a strong grasp on both sides.

What to say to the CIO: FUD is great for convincing the technical silo. They need to know their vulnerabilities. Here are some industry FUD MFA statistics that I have compiled from different sources to convince the technical silo:

- Cost of a data breach in the US: $225 per record. ***Source****: 2017 Cost of Data Breach Study: United States, Ponemon Institute, June 2017*
- The easiest and fastest way for hackers to get sensitive data is through access to Privileged Accounts (31%). Followed by email access (27%). ***Source****: Black Hat 2017 Hacker Survey Report, Thycotic, July 2017*
- According to 94% of the hackers surveyed, Multi-Factor Authentication is a big obstacle for accessing sensitive data. ***Source****: Black Hat 2017 Hacker Survey Report, Thycotic, July 2017*

- 85% of hackers surveyed agree that human managed security is the easiest security to break. That's because having humans remembering and changing passwords is the top cyber weakness. ***Source****: Black Hat 2017 Hacker Survey Report, Thycotic, July 2017*

- Logon credentials are one of the easiest attack vectors to exploit. ***Source****: Black Hat 2017 Hacker Survey Report, Thycotic, July 2017*

- 81% of hacking-related breaches leveraged either stolen and/or weak passwords. ***Source****: 2017 Data Breach Investigations Report, 10th Edition, Verizon, April 2017*

- 89% of companies in the US use User Name and Passwords for network logon. ***Source****: Gartner Group*

- Hackers target SMBs 70% of the time. ***Source****: US Department of Homeland Security*

- Of the SMBs that have a data breach, 40% will go bankrupt within 6 months. 85% within 2 years. **Source***: US Department of Labor*

- 60% of people use the same password for everything. ***Source****: Password Management Evaluation Guide for Businesses, Keeper, 2016*

- 90% of user generated passwords can be cracked. ***Source****: Password Management Evaluation Guide for Businesses, Keeper, 2016*

- The number one help desk call is for forgotten passwords and the annual industry cost for password resets is $10 billion. ***Source****: Gartner Group*

- 47% of employees in US businesses waste up to 15 minutes a week typing in passwords. ***Source****: User Productivity versus User Security: How to Strike the Right Balance, IS Decisions, 2016*

Long, complex passwords are a viable means of authentication. They represent the Knowledge (Something you Know) factor. However, the computer industry has put the weakest link in cybersecurity in charge of them – the user. You don't secure network data by removing passwords, but rather by removing the user from managing them. When you allow users to manage their own passwords, you just put them in the role of Network Security Administrator. The statistics above show that 94% of hackers view Multi-Factor Authentication as a very strong front-end defense.

Just because the CIO is convinced that MFA would be a strong deterrent against a network breach, it does not mean a sale is guaranteed. The CIO must provide the financial silo both the FUD relevance to their network and the financial benefits of implementing MFA to request additional money or increase next year's budget. Let's face it, cybersecurity products and services are typically not cheap. Asking for more money can be embarrassing and difficult for the CIO. It can make him look like he doesn't have a handle on the company's network requirements.

There are no silver bullets or single-point solutions that will make a company's network 100% secure. Security is accomplished through layering different technologies. MFA is often the most overlooked cybersecurity line of defense. MFA secures the virtual front door; similar to a door lock that secures

the physical front door. You need to lock both.

What to say to the CEO: I remember what Rich Dad guru, Keith Cunningham, once told me, "If you purchase something and it doesn't increase revenue or lower operational costs, then you purchased a liability. Too many purchased liabilities will lead to bankruptcy." Unfortunately, CEOs often view cybersecurity as another liability on the balance sheet. It's time to present cybersecurity from the asset perspective.

The role of the CEO is to put the company's policies, procedures and positionings in place to *enhance shareholders' value* by increasing revenues while managing costs. The three items they care about are: profit, profit, and profit. Profit is not a bad thing. Without it, there's no company, no employees, and no need for a CIO or computer network.

To understand how to sell into the financial silo, you need to know the three questions every business owner focuses on:

1. How will a new product or service increase my revenue?
2. How will a new product or service reduce my costs or increase productivity?
3. How will this product or service increase customers or make me a market leader?

Here's how MFA addresses each of these questions:

1. MFA Increases Revenue:

- If a company's R&D data for a new product is stolen by an overseas competitor who can bring a clone product to market faster and cheaper than you, how would that effect your revenue when you launch, assuming you could? The NSA Chief has stated, "Cybercrime Consitutues the 'Greatest Transfer of Wealth in History." If 94% of hackers view MFA as a deterrent, then MFA can combat premature price and profit erosion.

- In a 2015 Gallup poll, 70% of Americans are worried about identity thieves stealing their savings, tax refunds, social service benefits, and even their life. Security in the past was treated as an afterthought or third party add on. However, companies like IBM, Microsoft and Apple are putting security in the forefront of these products and charging more for their products and services. Customers are now willing to pay more for products with security.

- The theft of weak passwords accounts for 81% of all data breaches. Decreasing insurance premiums, law suits, government fines, customer losses and eliminating the redirecting of resources to damage control are just a few of the savings realized when you don't have to deal with a data breach.

2. MFA Increases Productivity:

- It has been shown that the time it takes an employee to type in their password to log in throughout the day adds up to 3-10 minutes per employee. It all depends on the number of accounts and the login-logoff frequency. This time adds up to thirteen to forty-three hours a year per employee. How many man-months is your company losing to logging in,

when it could be automated - and more secure?

- The most time-consuming activity of any IT help-desk is resetting passwords. Not only do you have to pay IT a salary to do something so trivial, but you are also paying an employee to sit around waiting, not doing their job because they can't logon to their computer or network. It is estimated that resetting passwords accounts for 40% - 70% of IT's help-desk time. The average employee down time is around 20 minutes per incident. Multiply that time by the frequency forgotten passwords occur, the number of employees, and their salary and you are talking serious productivity issues for something as simple as forgetting a password. Automating this process with an MFA enterprise password manager virtually eliminates this expense.

3. MFA Increases Customers:

- After a data breach, it is documented that the average number of customers who leave the attacked company is 30%. Customers are fed up with the way companies are poorly protecting their personal information. Whether you want to call cybersecurity flaws carelessness or stupidity, these breaches are having devastating financial and life-quality ramification on hundreds of millions of Americans.

- A company that positions itself as caring about their customer's personal information will attract new customers. New customers will come to you because of your security or because their previous vendor let them down. Either way, you will increase your customer base by letting them know you have MFA protecting them.

- Since 2010, it is estimated that 900 million Americans have had their personal data compromised. The actual US population is 324 million Americans in 2017. This 900 million basically means that every American's data has probably been compromised 3 times over the 7 years. When your competitor loses 30% of their customers, even if you would only be interesting to say 2%, that's 5.4 million potential new customers! If you have MFA in place.

- Word of mouth advertising is one of the best ways to get your message out. Especially with all the social media outlets available today. You know that a bad review can break a company, so why not make social media work for you by having raving fans. If one company can draw in new customers by advertising they have the "cleanest bathrooms", imagine what "protecting your data" could do.

Why Companies Need Power LogOn® Now!

Power LogOn is an enterprise password management and Multi-Factor Authentication solution. Power LogOn is being used by government agencies, healthcare facilities, schools and businesses around the world. We have customers as large as sixty-thousand users and as small as six employees. At Access Smart, we don't believe in the "Rip and Replace" sales strategy that many of our competitors push. Instead, Power LogOn leverages off the current employee physical access ID badges and computer infrastructure. By keeping the installation fast and the cost-of-ownership low, MFA gets implemented faster, which in turn reduces the risk of a data breach. Power LogOn's MFA

solution has the potential to prevent 94% of hacks at a cost of under $100 per employee. Companies need to implement MFA right away.

One of the biggest mistakes a company can make is waiting until they finish building out or upgrading a new network before addressing MFA requirements. Delays keep them at risk for a data breach and potential bankruptcy. Expensive back-end cybersecurity solutions are worthless when the virtual front door is left unlocked. Power LogOn can be fully implemented and deployed within a few hours. Keep networks and data secure during server and network modifications. Then, when the new network is available, all the existing Power LogOn configurations and passwords are quickly moved over with no productivity loss.

Vertical Markets Case Studies

Every market vertical is different and every business in that vertical is unique. Predicting exactly how Power LogOn addresses a CEO's financial concerns depends on how their business is structured. In the following requirements and outcomes shared from our many users, you may find similarities that match your business needs.

Education: A charter school in Washington, DC contacted us about 9-years ago regarding better password management. Their IT department had implemented secure network authentication with long, complex passwords that changed every three months. However, that increased security caused new problems and costs. For example, they had an increase in the number of password reset help desk calls, computers unavailable when a previous student improperly logged off the computer, and the need to hire more IT people to handle these issues.

The school implemented Power LogOn and their help desk calls dropped 70% while still maintaining their secure password policy. When the student removes their smartcard, the computer properly logs the user off, making the computer ready for the next student. IT personnel no longer were running around the school every 45 minutes to re-boot computers. Because Power LogOn resolved the password management issue, the school did not have to hire more IT staff. Overall, according to the IT Director, Power LogOn paid for itself within 9 months.

A side benefit that the school did not expect was the cost savings from student turnover. Power LogOn licenses are transferable. So as each group of students graduated or left, and new students enrolled, the old licenses were transferred to the new students at no additional cost. Because Power LogOn licenses don't expire, there were no annual renewal or subscription expenses to impact their budget.

Healthcare: Doctor offices, clinics and hospitals all must meet the HIPAA and HITECH government mandates. An HHS auditor stated that they are specifically looking for non-HIPAA compliant providers because they see the high fines as a new revenue stream for HHS. The cost of a Willful Neglect violation ranges from $10,000 to $50,000 for each incident and can result in criminal charges against upper management. The healthcare industry is keen on finding HIPAA compliant solutions to avoid these fines.

Recently, a hospital contacted Access Smart after suffering a data breach of patient records. Besides the expensive fines, law suits, and quarterly security audits, the hospital was required to

deploy MFA to every employee accessing electronic medical records (EMR). When the hospital IT Department understood the complexity of the different PKI MFA solutions on the market, they realized it would be another 18 months before they could satisfy the HIPAA requirement. IT needed a fast, affordable secure alternative. The hospital contacted Access Smart, purchased our Installation Starter Kit, and within two weeks had finished a full pilot program. Out of the box, Power LogOn easily integrated into their existing EMR software, other software applications, and Power LogOn worked with their existing 125 kHz proximity ID badges. With Power LogOn and other changes, that hospital got off the HHS watch list, the HHS quarterly audits were cancelled, and funds were diverted back into patient health care and operational costs.

For another very large hospital, both security and convenience were their primary concerns. In investigating different cloud-based password management services, IT was concerned about outsourcing their logon security and then becoming reliant on that service's security practices. For the hospital to keep control of their network security, the hospital required a centrally managed, on-premises, secure MFA password manager like Power LogOn. The IT Department is currently evaluating Power LogOn. The preliminary feedback has been very favorable with high praise for its convenience and flexibility to address multiple types of logon security.

A few years ago, a doctor wanted to secure his office network, and saw that MFA was a strong recommendation within HIPAA. Seeing that PKI was too expensive and complex for his small practice, that's when he investigated Power LogOn. At a fraction of the cost of certificate-based logon solutions, the doctor installed and set-up Power LogOn himself. The doctor was so impressed with Power LogOn that he wrote an article about his experience and recommended Power LogOn to his colleagues. Not only has Power LogOn satisfied his HIPAA compliancy issues, his staff found it very convenient to manage all the password logons.

Government: All employees of the US Government have either a Personal Identification Verification (PIV) or the military equivalent Common Access Card (CAC) credential. Some government networks require digital certificates to log in while other web sites, accounts, applications and networks still require a User Name and Password. Government agencies need secure authentication for both types of logons. Power LogOn meets their requirements.

Power LogOn allows fast deployment because it works out of the box with PIV and CAC credentials without any re-badging, re-programming or re-certifications. It has been independently verified by NIST labs to be FIPS 201 and FIPS 140-2 compliant. Power LogOn works side-by-side with the government's certificate based solution, giving IT the flexibility to integrate Power LogOn into their current infrastructure.

An additional savings was realized regarding the government's hiring of contractors. Contractors have a high employment turn-over. The standard PIV certificate credential became too expensive, especially because they must be destroyed when the contractor's term is up. Power LogOn's ability to transfer licenses means that an agency could purchase less expensive cards, not have to involve the DHS, and rotate licenses as contractors come and go. The cost savings to the government is substantial.

On a final note, Power LogOn also meets the Defense Federal Acquisition Regulation Supplement (DFARS) and NIST's 800-171 requirements for defense contractors. Without having to go through the

arduous task of purchasing CAC or CAC-Like credentials through the DHS, contractors are able to keep their contracts with the Department of Defense because Power LogOn makes them compliant on the MFA requirement.

Industrials: One of the ramifications from all the data breaches and attacks on corporations has been to push for stronger web and network authentication. Corporations have built out their Internet and Intranet to make doing business with them easier for their many suppliers. To reduce the risk of a data breach, these same corporations are now imposing MFA requirements on their suppliers. If a supplier fails to comply with cyber security procedures outlined by the corporation, they will be dropped as a supplier. This is a major financial impact for these suppliers. Power LogOn has allowed suppliers to show their compliance to security with an affordable MFA password manager.

While the four vertical markets mentioned above have benefited from Power LogOn, Power LogOn has also been deployed in the utilities, financials, insurance, retail, entertainment and many other verticals. It is appropriate anywhere cybersecurity and authentication is required. How Power LogOn will increase revenue, lower operational costs, gain new customers for your business is hard to predict. Every business is different. What we do know is cybersecurity has become a major requirement throughout every industry. It's not about how MFA cybersecurity will enhance shareholder valuation, it's about how not having MFA will lower your valuation! Power LogOn addresses the most important cybersecurity hole: secure, multi-factor authentication during computer, application, server and cloud logon.

As a reseller, when your customer requires cybersecurity products, the very first question you need to ask is, "How do your employees log in to their computers, network and applications? And when they answer, "With a User Name and Password." Your first recommendation must be Power LogOn.

The Take Away

The cybersecurity industry is too focused on the technical issues and not on the business issues. Maybe that's because engineers like to focus on solving problems and don't normally speak about ROI, Assets, Liabilities, Balance Sheets, or P&L statements. But that is the language of business. Until you can make upper management understand the profitability of implementing cybersecurity, and specifically MFA, it will always be a struggle to secure networks. Hackers will continue to capitalize on security holes and customers will feel betrayed by companies that lose their personal information.

As a sales person, you may have to sell to both silos. Understand that the arguments made for one group may have no value to the other. If you can only present to the technology side, be sure to arm the CIO with these business arguments so he/she can justify MFA expense to the CEO/CFO in a way they can understand.

Dovell Bonnett - "The Password Guy"

Dovell Bonnett has been creating computer security solutions for over 20 years. His passionate belief that technology should work for humans, and not the other way around, has lead him to create innovative solutions that protect businesses from cyber-attacks, free individual computer users from

cumbersome security policies, and put IT administrators back in control of their networks.

He has spent most of his career solving business security needs, incorporating multiple applications onto single credentials using both contact and contactless smartcards. The most famous example of his work is the ID badge currently carried by all Microsoft employees.

In 2005, he founded Access Smart, LLC to provide logical access control solutions to businesses. His premiere product, Power LogOn, is a multi-factor authentication, enterprise password manager used by corporations, hospitals, educational institutions, police departments, government agencies, and more.

Dovell is a frequent speaker and sought-after consultant on the topic of passwords, cybersecurity, and building secure, affordable and appropriate computer authentication infrastructures. His most recent book is ***Making Passwords Secure: Fixing the Weakest Link in Cybersecurit***y.