onelogin

WHITEPAPER

Solving the password problem in manufacturing

Protecting passwords is key to protecting corporate data and IP

Modern manufacturer's IT organizations get squeezed from all sides. Margins are tight, compliance requirements large, and they work within a globally distributed ecosystem of employees, partners, and suppliers.

To keep production lines moving, IT departments in manufacturing companies must make it easy for workers to access equipment quickly, even in challenging environments like the plant floor or in the field where employees might be wearing thick work gloves or other safety equipment.

Add to this the need to accommodate access through a wide variety of devices: laptops and tablets, mobile phones, controllers built into equipment, and ever-evolving IoT devices. Accommodating all these needs is a monumental task. Manufacturing IT plays a pivotal role in accomplishing it.

Compliance is costly—but a breach is even more so

According to Deloitte, 39% of surveyed manufacturing executives experienced a breach in the last 12 months. And the risk is growing. 82% of senior IT professionals predicted that unsecured IoT devices would cause a data breach in their organization, with 80% saying such a breach could be catastrophic.[1]

DATA BREACH ARE COSTLY:

- From a pure dollar perspective, the per-record cost has risen to $408, according to IBM and Ponemon.[2]
- The average cost of a breach is $3.86 million worldwide and $7.91 million in the United States.
- Of manufacturing companies that experienced breaches in 2017, 38% lost between $1 million and $10 million.[3]

One of the biggest impacts is lost intellectual property (IP). Losing IP or trade secrets can create an existential threat to a company. But even if a competitor doesn't use the knowledge to undercut the market, it can take a long time to recover.

Content

Whether at a desk, on the production line, or in the field, fast access to corporate resources is key. But you can't compromise on security.

[1] *"Change to Gil Press, "Cybersecurity By The Numbers: Market Estimates, Forecasts, And Surveys," March 15, 2018*

[2] *"Why Manufacturing Companies are Now More Susceptible to Data Breaches," Marsh & McLennan, 2018*

[3] *www.marshmma.com/blog/why-manufacturing-companies-are-now-more-susceptible-to-data-breaches*

In one survey, manufacturers reported that the **average diminished value** of the brand from lost IP was **18%**, and it took 8 months to restore the organization's reputation.

Most manufacturers must comply with regulations often aimed at preventing these kinds of breaches.

Compliance costs. A 2017 report from Ponemon Institute found the average cost of compliance for companies to be $5.5 million.[4]

But non-compliance costs more. The same study found that "the annual cost of non-compliance to businesses now runs an average of $14.8 million." Recent security breaches show what's at stake:

- FACC, an aircraft manufacturer and supplier, lost $54 million via an email attack.
- Apple discovered malware that had obtained sensitive information for 225,000 iPhone users.
- An ex-employee of Dupont downloaded 40,000 sensitive files to take to his new employer.

Investing in technology and procedures to protect your manufacturing organization is money well spent.

Non-compliance with regulations and resulting data breaches can cause you to lose certifications, clearances, and customers.

Passwords are the weakest link

Sadly, as an industry, manufacturing ranks in the bottom half when it comes to security, according to SecurityScorecard's 2017 report.[4] That's why passwords—and protecting them—are a focus in manufacturing IT as are many of the regulations for the manufacturing industry.

Regulatory legislation such as Sarbanes-Oxley (SOX) imposes requirements on information security, data access and segregation of duties (SOD) policies. These requirements include mature processes for access certifications and policy management to make certain policies are in place and adhered to.

It's no surprise that passwords are a focus for manufacturing IT—they're a focus for hackers, too. The most common attacks are aimed at obtaining user credentials, with the password being the critical element. That includes attacks like:

[4] *SecurityScorecard Security Research Team, 2017 U.S. State and Federal Government Cybersecurity Report," SecurityScorecard, August 24, 2017.*

- **Phishing.** The attacker uses a list of phone numbers or email addresses and delivers a message with a compelling call to action that sends users to a fake website where they provide their username and password.

- **Spear phishing.** The attacker targets a small group of individuals using well-crafted, believable messages that are relevant to the target group, often with personalized content. Again, a call to action gets users to provide their credentials.

- **Keylogger.** The attacker installs a program (often via a virus) that captures every keystroke on the user's computer, including sites visited, usernames, passwords, answers to security questions, and more.
- **Credential stuffing.** The attacker uses stolen credential pairs for one site on other sites, trying to gain access to many different sites.

- **Brute force and reverse brute force.** The attacker uses a program to generate possible username/password combinations to gain access. Or the attacker tries the most commonly used passwords (like Password123) on many different accounts.

- **Man-in-the-middle (MITM).** The attacker's program inserts itself into the interaction between a user and an app. The program then gathers the login credentials that the user enters—or even hijacks the session token.

Weak memories and too many passwords exacerbate the problem

Many of these attacks rely on the fact that users have to log in to too many sites using different passwords. So they tend to use the same passwords across multiple accounts. No wonder 72 percent of people have trouble remembering passwords[6] and 73 percent of online users use the same password across multiple accounts.[7]

Everyone in your ecosystem that uses a password presents a problem. That includes your partners, suppliers, workers, and even your customers. For example, 50 percent of employees don't create different passwords for work and personal accounts. If their personal password is compromised, your organization's data may also be breached.

Manufacturing IT often implements password rules—and enforces them with technology—to help ensure strong passwords. The most current recommendations include:

- **Require special characters.** Previously, a mix of numbers and upper and lowercase characters was recommended. But since users usually add numbers to the end of the password and use capital letters at the beginning of words, these patterns make passwords easier to predict.

In 2017, 81 percent of hacking-related breaches involved weak or stolen credentials.[2]

Manufacturers were targets for more phishing attacks than any other vertical in 2017.[8] Why?

- High ratio of production to office staff.
- Low frequency use of shared kiosks, meaning idle, vulnerable accounts.
- Poor employee awareness of how to spot phishing attacks.

[6] *"5 Obstacles to Employee Productivity," OneLogin.*

[7] *"TeleSign Consumer Account Security Report," TeleSign*

[8] *" Manufacturing a key target for cyber attacks," Computer Weekly, August 2017*

- **Require long passwords.** Password length has the biggest impact, and longer passwords offer greater protection. To help users remember them, suggest that they choose a pass phrase, like BrightBlue#25MileRoadM@P.

- **Don't require users to change passwords frequently.** Previously, the recommendation was that users change their passwords every 60 to 90 days, in case a hacker had obtained it. However, that just adds to the memory burden on users, making them more likely to use an easy-to-remember password or, worse, to write it on a Post-it Note or in a spreadsheet.

Although stronger passwords help, memory challenges with secure passwords remain a problem. That's why leading-edge manufacturers realize that the only way to truly close the password security gap is by adding two tools to the IT toolbox—single sign-on (SSO) and multi-factor authentication (MFA).

Setting password requirements, enforcing them, and educating users about common attacks make for a good start.

But these aren't nearly enough to protect your organization and data.

SSO and MFA are the golden keys to password security

Single sign-on and multi-factor authentication are critical to truly protecting IP and trade secrets because they address key problems with user authentication:

- Reduce the number of usernames and passwords that staff have to remember.
- Reduce the number of times that users have to log in—even when they need access to multiple apps or websites.
- Require additional information from a user, beyond passwords, to verify the user's identity.
- Make it easy for users to reset their passwords securely if they forget them.

Single sign-on. SSO is a system that lets users securely authenticate with multiple applications and websites by logging in once—with just one set of credentials. With SSO, the applications or websites that users access rely on a trusted third party to verify that users are who they say they are.

Multi-factor authentication. MFA is a security system that verifies a user's identity by requiring multiple credentials. Rather than just asking for a username and password, MFA requires other—additional—credentials, such as a code from the user's smartphone, the answer to a security question, a fingerprint, or facial recognition. (You may have heard MFA referred to by other names, such as two-factor authentication or two-step verification.)

Adding either one of these golden keys will help to lock up your organization's data and prevent unauthorized access. But adding them both will give you the best chance of preventing a breach.

SSO has many benefits

Single sign-on offers multiple benefits, while ensuring that users only need to sign in once with one set of credentials:

- Greater security and compliance.
- Improved usability and employee satisfaction.
- Lower IT costs.

Security and compliance with SSO are just the beginning

Every time a user logs into a new application or machine, it's an opportunity for hackers. SSO reduces the number of attack surfaces because users only login once each day and with only one set of credentials.

SSO helps to address government and industry requirements for effective authentication of users accessing sensitive data. Most SSO systems also provides an audit trail to track user activity and access. And any SSO solution should enable automatic log off, which is another frequent requirement for manufacturers working in highly secure environments.

SSO improves usability for staff

Maintaining separate usernames and passwords for each app or machine is a huge burden for your staff. Frankly, it's unrealistic. And when your workers are out on the floor in work gear that makes it hard to type, SSO is mandatory.

Single sign on reduces the cognitive burden on users. Signing in once saves time and frustration, improving worker productivity and satisfaction.

SSO lowers IT costs

Finally, SSO lowers IT costs by reducing password resets. When each app or machine requires a different username and password for every employee, the chances are high that employees will forget passwords, which means that help tickets to reset passwords pile up.

Not only does SSO reduce tickets because users have only one set of credentials to remember, but also it allows people to reset their own passwords, eliminating the need for IT involvement. That's especially helpful as part of a customer or supplier portal.

Not familiar with SSO?
Find out how it works.

See how SSO helped manufacturer Consort Medical.

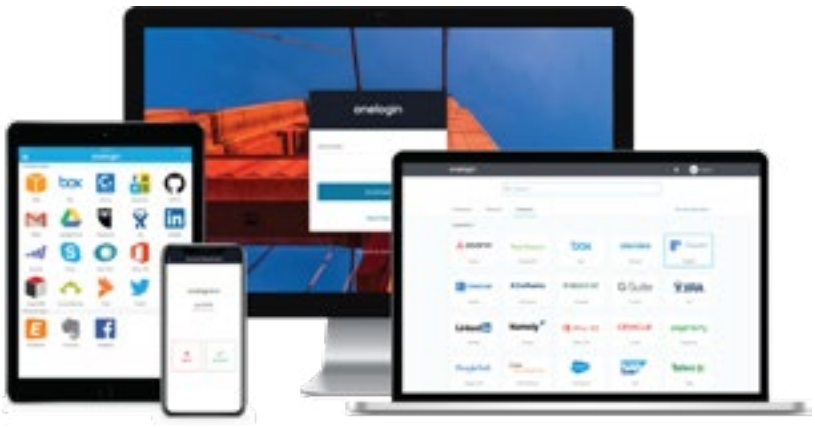
How does MFA help security?

MFA has become a widely accepted, critical component of security, because it takes access beyond passwords and requires users to further verify their identity. Those additional factors seriously frustrate hackers in their attempts to obtain login credentials.

Multi-factor authentication works to prevent successful attacks by requiring additional information or credentials from the user. A phishing attack may garner a user's credentials, but it won't provide the hacker with a fingerprint, for instance, or the answer to a personal security question. Similarly, a brute force or reverse brute force attack may manage to find a working username and password, but the attacker doesn't know which other authentication factors the MFA system will require and, regardless, won't have those credentials.

Similarly, MFA can combat more sophisticated attacks such as MITM by incorporating an additional layer of security. Even if the hacker or program inserts itself and captures the information that the user enters, you can set up MFA to require that the user supply credentials from a different device or channel. For example, a user logging in from her laptop may be required to use a phone app, such as OneLogin Protect authenticator, to send a code from the phone to complete the login. The MITM hacker doesn't have access to the user's phone, so the breach is halted.

Not familiar with MFA?
Find out how it works.



Devices, devices, so many devices
Your workers aren't just at a desk. They're on the floor, out at customer sites, out in the field, and even outdoors. They aren't carrying paper and clipboards. They're using laptops, tablets, mobile phones, controllers on machines, and special, connected devices needed for their work.

And that's fine. Both SSO and MFA work across devices. Workers can sign in—once—from their device to access all the apps they need. And it doesn't matter whether they're accessing the information from their phone, tablet, or computer, MFA adapts and asks them for the appropriate additional data to verify their identity.

Adaptive authentication can streamline workflow

SSO certainly offers a more streamlined experience, speeding up and simplifying login. But, since MFA requires that users provide additional information, can it negatively impact the production line or field workflow? Obviously, in emergency situations, such as when a production line needs to be stopped or a malfunction addressed, workers can't afford delays in access. That's where adaptive authentication comes in.

Adaptive Authentication adds transaction context and user behavior as key authentication factors, taking into consideration how users are trying to access the organization's resources.

Smart authentication systems know how a user normally works, such as where they work from, on which devices, and at what times. Behavior that's considered out of normal for a user can signal an attack. Adaptive MFA responds to the potential attack by requiring additional authentication.

Adaptive MFA helps streamline access, protecting that production line, because when you implement adaptive authentication in your organization, you determine the baseline login requirements for a given user or set of users. You might have stricter requirements for users in certain locales or for users in specific roles, and less strict requirements for others.

Each time someone tries to authenticate, the request is evaluated and assigned a risk score. Depending on the risk score, the user may be required to provide additional credentials or, conversely, allowed to use fewer credentials.

So, if a worker is using the tablet he always uses and is attempting to log in from the workplace floor where he normally works, he may only be asked to access via his badge. On the other hand, if the same worker tries to access a restricted machine with his username and password and that worker normally doesn't use that machine, he may be prompted to enter additional login information on his tablet. Or if a manager logs in from a geographical location far from her usual office, she may have to answer a security question.

Learn more about adaptive authentication

Conclusion

Manufacturing IT is in a tough spot when it comes to security. The demands from the bottom line, regulators, and the global ecosystem are high, but the cost of failure is even higher.

Shoring up some of the weakest links—passwords and authentication—is a relatively fast fix that adds significant protection against breaches, and two key technologies are critical: single sign-on reduces the attack surfaces of hackers, and multi-factor authentication adds protection beyond passwords. And adaptive authentication enables organizations to add security in a smart way that doesn't burden workers, suppliers, partners, and others or slow throughput and production time.

About OneLogin, Inc

OneLogin is the leader in Unified Access Management, Enabling Organizations to Access the World™. Businesses of all sizes use OneLogin to secure company data, while increasing IT administrator and end user efficiencies.

Implementation of our identity management solutions can be achieved in hours rather than days, delivering a fully featured administrative and self-service portal. Our ability to handle on-premises and cloud/SaaS applications makes us the identity-as-a-service vendor of choice for the hybrid enterprise. Multi-factor authentication, mobile identity management for one-click access on smartphones and tablets, and real-time directory synchronization all add an extra layer of protection.

Contact us to learn more about OneLogin.

www.onelogin.com/company/contact