

**Saltmarsh**

Saltmarsh, Cleaveland & Gund

CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS



**MARCH 2022**

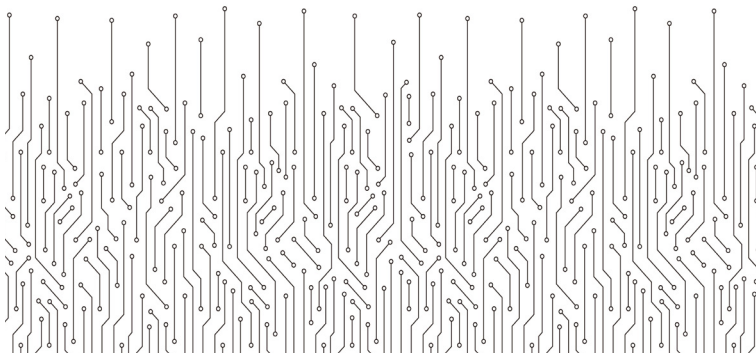
**MANUFACTURING OUTLOOK:  
LEVERAGING  
TECHNOLOGY TODAY**

**INSIGHTS FROM THE SALTMARSH MANUFACTURING TEAM**

# A COMPROMISED PASSWORD

A compromised password. That's all it took for hackers to take down the largest fuel pipeline in the U.S. last year, which led to gas shortages and higher fuel prices across the East Coast. The cost was even more for the cyberattack victim, Colonial Pipeline. It [has been reported](#) that Colonial Pipeline paid a \$4.4 million ransom to a Russia-linked cybercrime group and hired a cybersecurity firm to consult on its cyber defenses to help ward off future attacks.


As if manufacturers don't already have enough on their plates during this unique time facing unprecedented demand as well as labor shortages and supply chain challenges, they are being tasked with having to determine how technology can help them thrive while at the same time needing to protect themselves from possible cyberattacks. Let's look at both issues focusing on what manufacturers can do to leverage technology this year.



## Overcoming Labor Shortages

The Great Resignation of 2021 has left many manufacturers scrambling for employees. In addition to changing the way recruiting is done (discussed below), organizations such as Deloitte recommend automating recurring tasks and investing in Industrial Internet of Things (IIoT) technology within your manufacturing company. **According to [Deloitte's 2022 Manufacturing Industry Outlook](#), "45% of manufacturers surveyed expect further increases in operational efficiency from the IIoT's since they connect machines and automate processes."**

Deloitte notes that manufacturers who seek to capture growth and protect their long-term profitability should embrace digital capacities from corporate functions to the factory floor. Early adopters are transforming brownfield facilities with IIoT, robotics, automation platforms and artificial intelligence (AI)-enabled tools to support production, but the U.S. is not leading the way. Countries like Korea, Singapore and Germany have a larger number of industrial robots compared to manufacturing workers.



This may change soon, as the report says half of those surveyed expect to increase operational efficiency this year through investments in robots and cobots. In addition, investments in AI technologies are expected to see a compound annual growth rate of about 20% through 2025. However, human employees are still needed, and the old ways of recruiting them simply don't work well anymore.

Deloitte recommends manufacturers explore ways to add flexibility across their organizations to attract and retain workers. Those that can manage through workforce shortages and the rapid pace of change will come out ahead. Placing a spotlight on modern facilities, advanced technologies and career mobility is suggested to attract new employees and reach diverse and skilled talent pools.

How do you reach diverse talent pools?

Making online and in-person application easier and expanding outreach to systematically disadvantaged groups, and even adding the metaverse - a network of 3D virtual worlds focused on social connection - can help find talent and automate systems and processes.

**“ Investments in AI technologies are expected to see a compound annual growth rate of about 20% through 2025.**

# BEEFING UP CYBERSECURITY

Automation and adding new skillsets are two strategies manufacturers can use to their advantage to stay competitive. On the flip side, you can't forget about the increasingly sophisticated hackers out there that are ready for combat. Protecting your systems requires forethought and investing your time and resources.

According to a September 2021 article in [The Manufacturer](#), most U.S. manufacturers reported phishing or ransomware security incidents in the preceding 12 months. The [Deloitte 2022 Manufacturing Outlook](#) notes, "Cybercriminals can cause harm beyond intellectual property theft and financial losses, using malware that now ties in AI and cryptocurrencies. They can also shut down operations and disrupt entire supplier networks, compromising safety as well as productivity. A patchwork of regulations for different industries could be consolidated under the current administration's 'whole-of-nation' approach to protect critical infrastructure."

Regulations aside, all manufacturers should have a cybersecurity plan that starts with conducting a cyber risk assessment. This exercise will identify the biggest threats that affect the business and allow for the necessary steps to be taken to protect it. The quantified data produced in an assessment can help in the decision-making process.

In addition to identifying weak spots, a cyber risk assessment can also be useful for simplifying IT

systems and processes, something that makes it easier to review and improve existing security controls. According to a [report from Hartman Executive Advisors](#), this essential assessment step can help determine if preventive or corrective controls need to be enhanced or modified. Going hand-in-hand with a cyber risk assessment is an incident response (IR) plan that enables the detection and quick response to cyberthreats.

***An [IBM whitepaper](#) notes that nearly 3/4 of organizations don't have a consistent, enterprise-wide cybersecurity IR plan, despite the fact that those that do have an average data breach cost that's \$2.46 million lower than their planless counterparts.***

While having an IR plan is an excellent step to take, IBM notes it is also important in this day and age to have security professionals with extensive expertise on hand.

# THE TAKEAWAY

Manufacturers are being tested like never before by a conglomeration of challenges, including labor shortages and the potential of cyberattacks. Those that will survive and thrive will consider the benefits of

increased automation, the value of changing how recruiting is done and the necessity of a cybersecurity plan, including cyber risk assessments and an IR plan.



# HOW TO GET STARTED

The [manufacturing experts](#) on the Saltmarsh team are ready to share their expertise. Please contact us to discuss any existing and potential challenges you face as a manufacturer— let us help you ensure your successful future.



**SUZANNE COX**  
CPA, CIT

SHAREHOLDER

[SUZANNE.COX@SALTMARSHCPA.COM](mailto:SUZANNE.COX@SALTMARSHCPA.COM)



**CRISTINE TORREFRANCA**  
CPA

MANAGER

[CRISTINE.TORREFRANCA@SALTMARSHCPA.COM](mailto:CRISTINE.TORREFRANCA@SALTMARSHCPA.COM)



**STEPHEN REYES**  
CISA, CISSP

IT SHAREHOLDER

[STEPHEN.REYES@SALTMARSHCPA.COM](mailto:STEPHEN.REYES@SALTMARSHCPA.COM)

## JOIN OUR EMAIL LIST

TO RECEIVE QUARTERLY INSIGHTS

[SALTMARSHCPA.COM/MANUFACTURINGOUTLOOK](https://SALTMARSHCPA.COM/MANUFACTURINGOUTLOOK)

Saltmarsh is one of the largest locally-owned CPA and business advisory firms in the Southeast, serving clients throughout the U.S. and worldwide from offices across Florida and in Nashville, Tennessee.

The firm offers a full range of professional services, including a variety of specialized consulting services for many industries and high net worth individuals. We are an independent member of the BDO Alliance USA, which provides us access to national resources to better serve our clients. Saltmarsh has been recognized as one of Forbes' Top Recommended U.S. Tax and Accounting Firms, named one of the Top 200 Firms in the U.S. by INSIDE Public Accounting and a Regional Leader by Accounting Today.

### FOLLOW US

SALTMARSHCPA.COM

(800) 477-7458



**Saltmarsh**  
Saltmarsh, Cleaveland & Gund  
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS