ISSUE 56 SEPTEMBER 2022

RJ2 TECHNOLOGIES

Newsletter

What's Inside:

This month's perspective is brought to you by:
RJ2 Technologies President, Jeff Dann

It's Time to Use Automation to Improve Performance Levels

Workflow process can often be a critical element to improve efficiency but often overlooked by new business owners or small to medium-sized businesses. Most companies will focus on certain buzzwords like productivity and efficiency, but how do we get there, and how do we measure them? It all comes down to that workflow process.

Every employee starts their day in a habitual manner and depending on the industry, will have a typical order to their day and week at work. Since every business utilizes technology in some fashion to provide an advantage to your tasks and process to avoid wasting time. But few actually implement automation to properly utilize the technology to its fullest.

How does automation help employees perform daily routines to improve work performance? What are the overall benefits, not only for employees but also co-employees, customers and vendor depending on the role? Let's dive right in!

Automation Is...

It is typical for automation to improve performance levels, but what is it? Automation is the technology that automates time-consuming manual work to perform a specific task faster, more accurately and over long periods of time generate the same result. Some people may reference it as workflow automation or process automation; however, the overall function of any automation is the same. It is simply using different types of technology to carry out tasks automatically that can reduce cost, increases speed and accuracy.

Now, are there different types of automation? Certainly. It all depends on your company's needs. Every business is unique in some sort of way, shape, or form. This means that the way you do your daily tasks will also be unique. As your company grows, you want to ensure that your employees can perform to the best of their ability. Being productive and efficient are key elements in creating a strong business. Encouraging and building a communicative team are key factors in a creating a healthy workplace and culture. How can we tangibly acquire those key elements and factors? One incredibly helpful tool is by having a smart, healthy infrastructure in place with proper and adequate automation to improve performance levels. If you aren't sure how exactly to start that process, discuss options with your IT team, managed services provider, or contact a professional within this field.

Continued on page 2.

CONTINUED...

A quick rundown on important features to consider when choosing automation software and services for your company (in no particular order):

1. Access control
2. Participant alerts
3. Data security
4. Progress trackers
5. KPI reports
6. Regulation compliance
7. Easy-to-use builder tools
8. Clear workflows
9. Integrations

Keep in mind that you can use automation in all different departments and industries. Just about every organization needs to track data and keep records organized, which means that automation would be a beneficial tool no matter what. Accounting and finance departments can pull data from various documents to create charts quicker. Sales and marketing can contact clients, personalize product suggestions and post on social media with more efficiency and faster gathering of information to construct. Human resources can incorporate a more efficient and consistent onboarding process. All due to automation features that are customized for their needs.

An Employee's Work Performance

No matter who you talk to or what you read about automation, every person or blog will tell you that automation saves time. Since automation clears redundant tasks, your employees will save time and be able to focus on other revenue-generating activities. This is a huge win for small to medium-sized businesses! Time is incredibly precious, and if you're a business that is trying to grow, you likely feel the nonstop pressure of time ticking away. When you alleviate trivial tasks, this is how your employees can benefit from automation to improve performance levels. They will feel like they can get more done and give more input on how to strategize and grow the company with their team.

What are other ways that implementing automation to improve performance levels will boost morale and your workplace culture? For starters, it can help avoid burnout. One of the most common reasons that burnout happens is because people feel that they are being overworked or they feel that their time isn't being used as efficiently or effectively as it could. Working too hard and/or for too long leads to burnout, which in turn can lead to an employee quitting their job. How can we avoid this from happening? Reducing someone's workload even just by an hour a day can be a huge step in the right direction. Automation can also help avoid the type of burnout that some get by feeling bored of unfulfilled at work. It gives them time to focus on more important tasks or projects rather than solely on the monotonous tasks. It may sound silly and like it's too good to be true, but automation can do wonders for your employees.

Benefits For All:

Automation To Improve Performance Levels, Prices, Time Management & More

What else can automation do? There are benefits that can be reaped from all sides - employee, employer, consumer/customer, and your business overall. Automation reduces human error. It improves operational efficiency and increases scalability. Overall, one of the best benefits is the ability to save money. Saving money allows your business to stay competitive in price points as well as reducing costs in other areas. For example, you can save in terms of time and resources such as money you would spend on paper, ink, envelopes, employees time, etc., throughout a year's time by automating and performing more electronically.

It's time to discuss communication within your company and teams. When you are able to use automation for communication purposes, you will streamline communication between team members, departments, and your business overall. Miscommunication is inevitable; we are all humans. However, in the workplace, a lot can go awry with poor communication routes in place. Employees and customers often cite poor communication as a stressor that makes them want to leave. When you decide to implement automation to improve performance levels, you may as well invest in automation within your communication structure as well. You can even eliminate team members having to remind others when to have something done. How? They can receive reminders automatically. This is the magic of automation. You have increased communication, increased accountability, cost savings, efficiency, productivity boost, empowered employees, higher-quality work, improved customer experience and satisfaction, and on and on we can go.

Conclusion

If you want more information regarding automation to improve performance levels and options that will benefit you and your organization, contact us today. Consult with a managed services provider that cares about their clients, works as an extension of your team, and provides quality services. Regardless of your business size, the benefits of a long-term relationship with a knowledgeable and reliable provider are essential for creating a thriving company. RJ2 Technologies will provide that to you.

Back to School! The 4 Cyber Security Trainings You Must Do With All Employees

The back-to-school season is here. For your employees and children alike, this is a time to refresh the information they learned last year and ensure that they were able to retain it. There's nothing wrong with needing a refresher, and this is true for both students and your employees.

If your employees have not recently taken a cyber-security refresher course, now is the time to provide them with updated information. Your staff needs to understand how to defend your company from potential threats. A cyber-secure culture can be created only if everyone buys into its importance and understands the potential dangers.

Cyberthreats come in many forms, but human error is the leading cause of cyberattacks. If your employees do not undergo cyber security refresher training at least once a year, they will be vulnerable to phishing e-mails, weak passwords, unsafe browsing and other types of cyberattacks. Additionally, in many cases insurance won't cover your claims if your employees have not undergone regular training. Finally, customers usually don't want to do business with a company that isn't keeping their information protected. It doesn't matter how big or small your business is – you must make an effort to ensure that all of your employees have gone through cyber security training. To help you get started, we've put together a list of the most important topics to discuss when training your team on cyber security.

Password Security

Most employees have a login to access the company's systems, data or Internet. When selecting passwords for these logins, employees should use strong passwords with letters, numbers, punctuation and special characters that are not shared between accounts. Employees should regularly change their passwords as well. You can also use multifactor authentication so you will know that those logging into an account are who they claim to be.

E-Mail

Employees should be wary of e-mails that come from outside of the company. They should not open any e-mails from people they do not know or have not communicated with in the past. Unless they know exactly where the e-mail has come from and are certain it is safe to open, they should not open any links or attachments within it.

Social Media

Some employees may have personal accounts set up through a company email address. Employees should be cautious about what they post on social media and shouldn't disclose private information about your company or your clients. If they did, it could be devastating to your company's reputation as well as your cyber security.

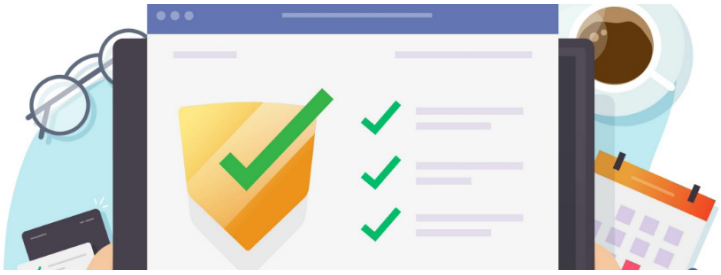
Protecting Your Company

Your company's cyber security practices are in place to protect company and client data, and your employees have a legal and regulatory duty to protect sensitive information. A reckless disregard for protecting company information can quickly cause your company to go under and has the potential to bring forth lawsuits. Establishing strong cyber security practices, training employees on those practices, and implementing them through technology, is the best way to protect your business from cyberthreats.

Featured Partner:

There's no easier way to use multi-factor authentication (MFA). Designed for the modern workforce and backed by a zero-trust philosophy, Duo is Cisco's user-friendly, scalable access security platform that keeps your business ahead of ever-changing security threats.

Tips for Safely Browsing the Web:



Even if your employees are only surfing the web, they are still vulnerable to various types of online threats, especially when working from home, using multiple devices, or connecting to different networks. It is recommended that you as the business owner put browser security measures in place to reduce the risk of potential data loss.

Install Anti-Malware Software

Most browsers have now been programmed to block websites with malicious content, i.e., websites that can deliver malware to your systems. The downside is, that even the most advanced browser cannot block all the malicious web pages out there, especially if a website is legitimate but has been converted into an unwitting mule for malware.

Since browsers blocking all malware infections from websites seems to be impossible, it is crucial that you install anti-malware software on every device used by you and your employees. This software will work to protect you from known viruses, worms, and other malicious software that are designed to capture your data and severely damage your IT systems.

Have Everyone in Your Organization Use a Virtual Private Network (VPN)

Hackers can pry into your internal channels and external communications with your customers and business partners to steal sensitive information, such as account login credentials and banking details. Lucky for you, you can use a VPN to encrypt your interment traffic. Essentially, a VPN will block any unauthorized party from being able to read any messages you or your staff sends out and receives via a web browser or another medium.

Install Ad Blockers

While most online ads are not harmful, some of them will collect and send your data to third party sources that will then send you more targeted ads based on the data extracted about you. Also, clicking the links on some of these ads will bring you to malicious sites. Thankfully, you can install an ad blocker that will help to keep away suspicious pop-ups and banner ads from showing up on your browsers.

Stop Online Activity Trackers

If you don't want to be monitored by third parties while you are on the internet, you can use private browsing mode, such as Private Browsing on Safari and Incognito on Chrome. Private browsing will also protect you from types of malware and cookie tracking. You can also use browser extensions that stop social networking sites, such as Facebook and Twitter, from tracking your online behavior and collecting other information about you. Such browser extensions include Privacy Badger and Ghostery.

The simple act of surfing the internet has become a recent concern regarding the amount of information companies collect and the constant threat of cyber-attacks. If you don't have sufficient protections in place to protect you and your employees, your data and your company could be at a severe risk. If you don't have any protections in place or are looking to improve your current defenses, fill out the form below to get in touch with our team of experts. We will start working as soon as possible to protect your company from all the potential cyber threats out there. regarding the amount of information companies collect and the constant threat of cyber-attacks. If you don't have sufficient protections in place to protect you and your employees, your data and your company could be at a severe risk. If you don't have any protections in place or are looking to improve your current defenses, fill out the form below to get in touch with our team of experts. We will start working as soon as possible to protect your company from all the potential cyber threats out there.

Why Cybersecurity is Important for Small Businesses

Introduction

Cybersecurity has been a hot topic for years, but it's always been a kind of abstract threat. Our smartphones weren't designed with security in mind; they were designed to be easy to use and carry around with us all day. As technology becomes more and more integrated into our lives, it's important that we all take steps to protect ourselves from cyberattacks like phishing scams or ransomware attacks.

In this article, I'll discuss why small businesses should invest in cybersecurity technology and training for both their employees and themselves regardless of whether they've ever experienced an incident personally.

Cybercrime is on the Rise

Cybercrime is increasing at a rapid pace. The FBI has reported that in 2017, there were nearly 1.4 million victims of cybercrime in the US and UK alone. And this problem isn't going away—it's only getting worse as more devices are connected to the Internet and attackers find new ways to exploit them for financial gain or other nefarious purposes.

In addition to directly affecting businesses, cyberattacks can have indirect effects on businesses as well: consumer confidence can drop because of news reports about attacks on retailers, disruption of supply chains can lead to shortages or higher prices for consumers at retail outlets, etc.—you get the idea!

As cyberattacks become more common and sophisticated, businesses will need to take steps now to protect themselves. This could involve creating a data breach response plan that outlines what happens when an attack occurs—for example, how does management notify customers about the situation? Should employees be told not to talk about this on social media? What steps should management take immediately after a breach has been confirmed? These questions should all be answered ahead of time so there's no panic or confusion later.

Hackers are targeting small businesses

Small businesses are often targeted because they are less likely to have the resources to defend themselves.

A small business may not have an IT department, or a dedicated security team. This means that there's no one on hand to monitor for suspicious activity or keep up with the latest vulnerabilities and patches. Small businesses also frequently lack information security policies or adequate oversight by management. In these scenarios, hackers can gain access easily without much resistance.

Fortunately, there are ways you can make yourself less of a target:

Implement a strong password policy and use multi-factor authentication wherever possible. Use a VPN when connecting to public wireless networks such as those at coffee shops or airports. Recognize phishing attempts and don't click on links or open attachments in emails from unknown senders. Install updates and patches for software as soon as they become available. Install anti-virus software and keep it up to date. Train employees on the basics of cybersecurity and do periodic audits to ensure the policies are being followed.

This is a good start, but it's not all you need to know. The best way to protect your business from hackers is by hiring a cybersecurity expert who knows how to prevent attacks before they happen.

Many businesses aren't keeping their employees up to date on cybersecurity training and education

As a business owner, you want to ensure that your employees are protected from cyber threats. But according to the Ponemon Institute, many businesses aren't keeping their employees up to date on cybersecurity training and education.

It's important for your company's security that you provide regular cybersecurity training for your staff members. This can include:

- Employee awareness programs
- Regular security checks
- Training sessions regarding new trends in cybersecurity (for example, phishing scams or new types of malware)

Employees can help protect themselves by: Staying up to date on new cyber threats Learning how to identify phishing emails and other types of scams Avoiding public Wi-Fi networks, which are often unsecured and easy targets for hackers Using strong passwords (including uppercase letters, lowercase letters, numbers, and special characters) that are changed frequently Asking you or your IT department if they have any questions about cybersecurity policies.

Tech Tips of the Month:

- Change your passwords every three months. Make them strong and DON'T use the same password twice
- Use a secure file sharing solution that encrypts your files while in transit to prevent eavesdropping and unauthorized users from accessing your files.
- Remove adware from your systems. Adware collects and stores data about you to target you with more personalized ads. To maintain more privacy, try using an adware cleaner to removed unwanted programs from running on your devices.

Continued on page 6.

CONTINUED...

Many Workers Aren't Practicing Good Cybersecurity Themselves Outside of Their Jobs

While it is important to be aware of the dangers of phishing and ransomware, it's also important to practice good cybersecurity yourself.

- Don't click on links in emails.
- Don't open attachments in emails.
- Don't visit websites that are suspicious, even if they look like Facebook or other trusted sites.
- Don't give out personal information on social media or via text message (this includes your address, phone number, credit card number, etc.). If you have a business email account for work purposes only and you want to share your personal information with

While cyberattacks may be increasing in frequency and intensity, there's a lot you can do to protect your personal information, your business and your devices. Investing in cybersecurity technology and training for both you and your employees is an investment in the health of your business now and in the future.

Conclusion

If you're looking to improve your cybersecurity practices, we've got a few recommendations. First and foremost, make sure all of your employees are aware of the risks associated with cybercrime. Doing this will help keep them more diligent about practicing good security on their devices and networks at home as well as at work. It's also important for each person involved in running the business – from top-level decision makers down to key employees – to be educated about what types of attacks exist so they know how best to protect themselves from them.

Finally, don't forget about yourself! Many people overlook their own personal information when it comes time for companywide training sessions or updates on new threats; however, having knowledge about how hackers operate can go a long way towards keeping yourself safe from any potential attacks against your personal data.

RJ2 SPOTLIGHT

Jack Creager
Systems Engineer

Jack has been in the professional filed since 2016. He is a Computer Science graduate from the University of Illinois - Springfield. Jack started his career in the IT filed working for Forsythe Technology in Skokie, IL. Before coming to RJ2 Technologies, he was a Program Operations Leader of Software and Licensing at GE Healthcare in Chicago. Jack recently joined the RJ2 family in July of 2022.

Fun Fact: Although a terrible golfer, Jack on average hits as far as the top PGA golfers, directly at any nearby water.

Where's your favorite place in the world?
- The golf course

What do you like to do when you aren't working?
- At home consists of hanging out with friends and family while playing yard games and grilling/cooking. I also enjoy playing a lot of different sports, fitness, and traveling to different places to go on hikes with my girlfriend and dog followed by trying that area's breweries.

What is the best career lesson you've learned so far?
- Change is the only consistency.

If you could meet anyone in the world, dead or alive, who would it be and why?
- Larry David because he is the king of comedy.