IT Strategy Brief

ISSUE 11 | VOL 6 | November 2020

INTEGRATE SEAMLESSLY

SWK MANAGED CLOUD SERVICES

"Useful Technology News and Ideas for Your Business"

What's Inside:

US Treasury Bans Ransomware Payments Based on Sanctions

Divisions of the US Treasury Department released an advisory in 2020 effectively implementing a ban on ransomware payments to groups under sanction by the American government. As quite a few of the gangs that specialize in this type of malware attack often act as nation-state hackers as well for their home countries, this order intends to severely cut down the possibility of supporting them. It also more strictly regulates the ability of certain cybersecurity firms to act as money handlers for payments to cybercriminals, which some had been doing discreetly while advertising other solutions.

Here are the top factors to know about the potential ransomware payment ban and how it can affect your business:

Specifics of the US Treasury Advisory
On October 1, 2020, the Treasury put out a press release announcing the advisories from two of its divisions that explain the details of the decision as well as the thinking behind it. The Financial Crimes Enforcement Network (FinCEN) and the Office of Foreign Assets Control (OFAC) each issued separate but similar statements ("Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments" and "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," respectively).

Within their acting powers given to their respective offices, both divisions made clear through their advisories that any transactions with a sanctioned party or parties could constitute a violation of US law. Various regulations come into play for this process, from data privacy reporting obligations to the act of facilitating a payment for a ransom, and finally the transactional contact with a party under US sanction. This is also why insurers and cybersecurity firms that end up handling money for or otherwise facilitate these payments are coming under extra scrutiny by the Treasury.

Ransomware Payment Ban Strategy Growing
This is not the first attempt to regulate these types of activities, with the NY State Senate trying to pass a bill earlier in 2020 that would effectively ban ransomware payments. However, this may be the beginning of a federal mandate explicitly prohibit ultimately contributing to cybercriminals that perpetuate this type of extortion. This method has evolved in recent years and even gangs that have historically relied on other techniques have increasingly migrated to encrypting files.

Nation-State Hackers and Cybercrime
Cybercriminal syndicates are active all around the world and have exhibited various levels of sophistication, but it is thought the most increasingly prolific are those based out of Russia. North Korea is another suspected culprit of employing nation-state hackers for collecting ransoms to achieve their objectives. Iran is not necessarily a repeat offender, but the SamSam ransomware which hit Newark in 2018 was traced by the FBI to two Tehran residents that primarily targeted the US and may well have acted for nationalistic reasons.

Continued on page 2...

What our clients are saying: Beth Ward Studios

"SWK Technologies has been very reliable for me. I needed help with my thermal printer and they called me right away to fix the problem. They have always managed to find a way to fix an issue in time for me."

Jerry Ramirez
Shipping Manager
beth ward studios

BETH WARD STUDIOS

Two ways to WIN a gift card!

It only takes a minute and YOU could be our next winner!

Last Month's Contest Winner:

Lori Lynch
Foundation Title

Please complete our brief survey in order to be placed in the running to win this month's gift card prize!

1. What do you like most about our services?

2. Tell us about a specific experience with us that you were happy with.

3. What are the biggest benefits you've received or experienced since hiring us?

4. What can we improve?

Email Jon Stiles (jonathan.stiles@swktech.com) with your responses
OR
Fill out our online form: http://bit.ly/nwsnews-survey before **Dec 6th** to get your name in the hat.

You could win a $25 Gift Card!

The Difference Cybersecurity Makes in the Cloud

Cybersecurity makes all the difference when working with the rapidly proliferating cloud technology organizations increasingly rely on throughout the world. Computing and network assets are gradually migrating to remotely-hosted deployments in popular consumer spaces, and browser-based user interfaces (UI) are being adopted at growing rates. Yet this aspect of digital transformation is moving faster than the ability of traditional IT processes to protect against new vulnerabilities that appear, or that of users to adjust to their role in the modern attack surface.

Cloud security has escalated the need for good education and expertise in endpoint protection, but above all, it has raised the demand for dynamic human intelligence. Hackers have proven that they can exploit conventional automated solutions like antivirus software by taking advantage of the gaps in code and with enough persistence. Defending your hosted environment against attacks requires dedicated monitoring and stewardship available in real-time for your critical data assets that can be exposed in the event of a breach.

Here are the top ways that human-driven cybersecurity makes a difference in the cloud:

Cloud Security Requires More Just Antivirus
Automation delivers incredible value for consolidating or outright eliminating manual tasks, but if there is any downside, it is that the technology still needs human input for improvement. Antivirus software can perform functions and hunt down malware faster and with more precision than any human, but can only do as much as it is programmed to. Hackers are using their own tools to get ahead of patch updates, and to exploit the areas where your firewalls cannot protect your users completely - human error.

Hosting in the Cloud Has Enabled Work from Home in the Pandemic
COVID-19 social distancing made the value of cloud networks readily apparent, and the spread of this technology allowed business continuity plans to be leveraged at an unprecedented scale. Unfortunately, many traditional IT resource deployments have still not been fully adapted to the reality of hosted infrastructures. As the business world sees increasing benefits from working from home, future strategies must include cloud security as a top priority for the distributed workforce.

Remote Work Is the Future but Will Stretch IT Resources
In the immediate and far-off futures, many companies will continue to operate with a significant enough portion of staff working remotely to make it a cybersecurity item. Many in-house IT departments will be stretched past the breaking point trying to monitor all the external access points in their network, and even outsourced managed service providers (MSP) will come up short without the right level of expertise and endpoint protection. You will need experienced cyber veterans familiar with hacker footprints to quickly and decisively deal with potential data breaches.

Legacy Technology is Not Built for Digital Transformation
Legacy software and hardware still often occupy a space in both business and consumer networks, and this creates gaps in cloud security where the technology designs clash. ERP rushed into SaaS development are a great example of the vulnerabilities that can slip through the cracks, but what can also be overlooked are all of the personal devices with access to your critical data that are not updated for the latest cyber threats. Without consistent monitoring for these weaknesses, your remote connections can be breached too discreetly to cause alarm until it is too late.

The Role of Cloud Service Providers
As the case with Capital One's data breach illustrated, enterprise cloud service providers (CSPs) like Amazon Web Services (AWS) place the responsibility of user security strictly on the customer. For midmarket and SMB hosting services, your business has to contend with this and the fact that you will be at the mercy of their uptime performance. If you migrate to a digital infrastructure with a CSP that does not have both a good record and a stated commitment to cybersecurity, then the protection of your data hosted online will be entirely reliant on you and your team.

Human Cybersecurity Intelligence Provides Dynamic Protection
The social engineering deployed by hackers relies on many of the same principles as traditional espionage, and your cloud security should be able to match this thinking in practice. Human cyber intelligence coupled with deep experience can uncover and react to threats in real-time, the same maximum speed the cloud operates at. This give you much more flexibility to leverage your IT resources and data delivered through hosted connections, and defend any overlooked backdoors within your network.

Continued on page 3 ...

Shiny gadget of the month: BusyBox - Smart Sign For Interruption-Free Work

By now just about everyone has either worked from home, or is still working from home. While the benefits of working from home can be great, it is not without some drawbacks. Even if you are fortunate enough to have secured your own office space for working from home you can still be faced with distractions and interruptions from others in your household. It can be particularly inconvenient if you are in the middle of an important call or just in the zone. There is a new gadget currently in funding that aims to put a stop to that for you. The gadget is called the BusyBox, and it is here to help with your working from home (or even in the office) needs.

BusyBox is a simple, but effective concept. Have a sign that signals to others that you are busy. The message is further emphasized by lighting up to let others know that you are occupied, much like an "On Air" sign at a radio station. Depending on which model you want it is more robust than just a light up busy sign. There is a digital version which has an LCD screen that you can use for custom messages and emoji's. Then there is a standard model with pre-printed slide in signs that use LED lighting to illuminate with the color and brightness of your choosing. Both options are connected and controlled via an app for your mobile device. They do have a button that you can purchase that you could place on your desk to toggle the box as well. The boxes are also rechargeable and come with two different style covers, charging cables, and a wall mount.

While to some it may seem silly to need a sign, to others it may sound like the perfect solution. If you were able to mount on your door, or even in another room of the house where people would be able to visibly see if you are busy it can prevent a lot of interruptions. Especially now with more and more people using video conferencing and other things where headphones may be used you don't always know if someone is in a live video call where you might accidentally walk by or be calling for someone. As mentioned before it could still be useful in an office setting for the same reasons. Everyone is probably all too familiar with having someone walk up to them and start talking not realizing you are on a call or focused on something.

Right now the BusyBox is estimated to start shipping in December 2020. There are still early bird options available on their funding page https://www.indiegogo.com/projects/busybox-smart-sign-for-interruption-free-work#/. The Digital version is going for $179 , the Standard for $69 and the Button for $25. It is a creative idea and will be interesting to see how it is adopted. They have surpassed their funding goals and are getting ready for production. Would you use one of these? Tell us what you think.

US Treasury Bans Ransomware Payments Based on Sanctions

Continued from page 1 ...

Cybersecurity Services Paying Off Ransoms
A new internal industry has emerged within cybersecurity where certain firms will handle the negotiation and payment for ransomware, or pretend not to and do it at inflated price. However, the US Treasury has made clear that now any party that does so must be registered for the service, which adds reporting and visibility requirements that could transform how this sector operates. Previously, cyber insurance companies were more likely to prompt their clients to just pay the ransom - now that such action is under the regulatory microscope, this may change.

The Safest Solution is to Backup Data
To clarify, this advisory does not perpetually ban ransomware payments, but what it does do is create huge risk for working with a party who may or not be under sanction and open you up to huge noncompliance fees. The safest solution for fighting against hackers is still to do everything in your power to prevent a breach, and backup your data regularly for if and when the worst scenario occurs. Only a sophisticated, frequent business continuity solution can protect you from being at the mercy of cybercriminals and limit the damage done by a malware infection.

Backing up Data Ensures Business Continuity Against Ransomware
SWK Technologies has firsthand experience with enabling businesses to restore their system and recover their data completely after a disaster. We will be able to help you find the right business continuity solution that works with your current software, ensure that it is consistently up to date and aid you in migrating recovered files back into your database to restore your network uptime.

Download our ebook here to discover more about ransomware and how to protect your business by backing up your data.

The Difference Cybersecurity Makes in the Cloud

Continued from page 2 ...

Deploying SOC as a Service
A security operations center (SOC) is a fully-staffed cyber intelligence and network monitoring unit dedicated first and foremost to proactive cybersecurity and incident response. Engaging a SOC as a service allows you to implement cyber defense at the operational level and deploy practical, technology-agnostic information security strategies across your software and IT stack. Being able to leverage a team of expert analysts and professionals for protecting your hosted infrastructure ensures that your business can cybersecure your communications down to the user level and mitigate external exposure.

The Benefits of Cybersecurity for Cloud-hosted Data
Whether you are aware or not, your data likely is exposed to a cloud endpoint - your smartphones, your Microsoft 365 apps, the websites you visit and more are either designed or being modified for SaaS connectivity. The only way to protect your system as well as ensure regulatory compliance for consumer privacy is to deploy cybersecurity that can handle modern network demands. Armed with the right solution, you will be able to take full advantage of the steady migration to cloud-hosted digital resources and position your business for maximum ROI on your software.

Leverage the Smart SOC with Secure Cloud Hosting
Secure Cloud Hosting by SWK Technologies allows you to implement a military-grade "Smart" SOC for your mission-critical business applications and network. With active IT support and endpoint protection delivered through our Managed Cloud Services division, you will be able to enjoy the true benefits of your technology stack while keeping your data cybersecure.

Contact us today to learn more about implementing cybersecurity with your cloud-hosted environment.

Gift Card Trivia!

This month's question is:

What is a safe solution to counteract Ransomware? (Hint: The answer is in this newsletter.)

a. There is none
b. Pay the Ransom to recover data
c. Business Continuity
d. Using a VPN

Please email Jon Stiles (jonathan.stiles@swktech.com) with your answer by **Dec 6th,** in order to be placed in the running for this month's gift card prize!

We can help you with:

- Cybersecurity
- IaaS
- Complete network management and support
- Troubleshooting and problem solving on all PCs and Macs
- Cloud services and virtualization
- Hardware installation and support
- Virus / spyware removal and protection
- Security solutions
- Employee awareness training
- VPN (Virtual Private Networks)
- Remote access / Mobile computing
- Server installations and upgrades
- Spam filtering
- Hosted email
- Web content filtering
- System backups, on-site and off-site
- Help desk

Contact us

Give us a call for more information about our services and products.

SWK Technologies, Inc.
South Jersey
650 Grove Road, Suite 106
West Deptford, NJ 08066

North Jersey
120 Eagle Rock Ave., Suite 330
East Hanover, NJ 07936

Phone: 856.956.5800
Fax: 856.845.6466

Visit us on the web at www.swknetworkservices.com

SWK
MANAGED CLOUD SERVICES

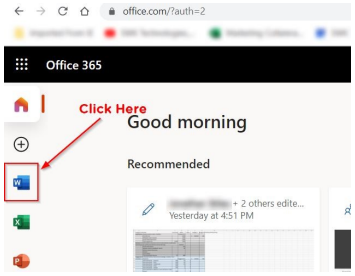
6 Microsoft Word Tips to Boost Productivity

As Microsoft Word remains one of the most popular business apps today, SWK Technologies is here with more tips to boost your productivity as well as save time on repetitive tasks. As an experienced Microsoft 365 and Office 365 provider and partner, our Managed Cloud Services division can help you use this application suite to its maximum potential on Windows and Mac devices. Discover how to get the most out of your documents and take advantage of the latest updates with this guidance.

Here six tips for boosting productivity in Microsoft Word:

Never Lose Work with Microsoft Word Online

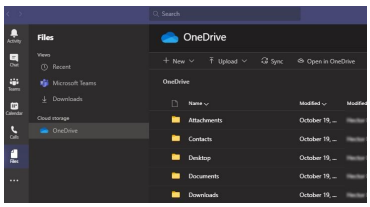
Even if you do not have the app installed in your local machine, you can still access Word on any computer, tablet, or smartphone device by going to Microsoft 365 Online. Go to www.office.com, sign in with your Microsoft account, and open **Word Online**, the browser version of Word.



By utilizing the **Share** button, your colleagues can access your document using Word Online or the Word app, which means anyone with the link and an Internet connection can jump right in.

Work on Files Collaboratively in OneDrive and SharePoint

You and your colleagues can work on and edit the same Word document at the exact same time by taking advantage of Windows hosted online. Your documents can be saved manually or automatically to the cloud and accessed through your company's Microsoft 365 or Office 365 database simultaneously.



Using **OneDrive**, click **Share**, then copy the link and send it to another user within your system. People with the link can view and edit the document in either the desktop app or online, and you can modify permissions when generating the link to prevent unwanted changes.

SharePoint also provides an interactive library for all of your organization's files, connected to individual OneDrive accounts or shared directories. These databases are also accessible through your Microsoft Teams account and can be found under **Files**, and uploaded or linked to in your channels under **Teams > Your teams**.

Track All Changes and Document Edits

Use the **Track Changes** function to monitor all edits made to your documents. Microsoft Word lets you monitor all edits that anyone makes to your document, so that you can go through the changes and accept or reject them accordingly. To turn on Track Changes, click on the **Review** tab then select **Track Changes**. When reviewing a colleague's edits, click on **Accept** or **Reject** as you see fit.

Do Quick Research with Smart Lookup

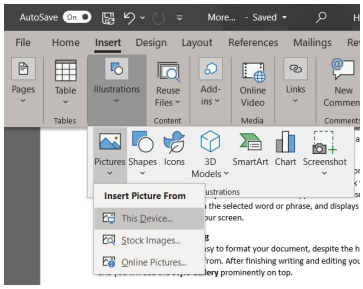
The Smart Lookup feature helps you do online research while you're working on a document — no need to open another tab and type in a query. Simply highlight and right-click the word or phrase you want to look up, and select **Smart Lookup** from the menu that appears. Word uses Microsoft's Bing search engine to conduct a search on the selected word or phrase, and displays the results in a pane that appears on the right side of your screen.

Word Document Formatting

The **Styles Gallery** makes it easy to format your document, despite the huge number of font types, sizes, colors, and effects to choose from. After finishing writing and editing your document, click the **Home** tab and you will see the **Style Gallery** prominently on top.

1. Select the text you want to format as a new style (e.g., a heading or a certain phrase).
2. Specify the formatting you want on the mini toolbar that appears. For instance, click Bold and Red if you want the text to appear as such.
3. Click the More arrow in the lower-right corner of the Styles gallery. Select Create a Style. This will open the Create New Style from Formatting dialog box.

Give the style a name and click *OK*. Your new style will appear in the Styles gallery, ready for you to use anytime.



Insert Images Fast

Word makes it easy to add images to your document without having to go looking in a browser. Just place the cursor on the area where you intend to insert the photo, click on the **Insert** tab, go to **Illustrations**, **Pictures** and select **Online Pictures** (type "clip art" on the search box if that's what you need), select a photo, then click **Insert**.

Edit a PDF

To edit a PDF in Microsoft Word, click on the **File** menu, select **Open**, and choose **Browse**. Highlight the file you want to edit, then click **Open**. Word will convert files to the new format using text recognition, so double-check if the conversion is correct. Make the appropriate changes, then click **File**, then **Save As**, then **Browse**. A "Save as type:" dropdown menu will appear at which point you will choose "PDF" then click **Save**.

Learn More Microsoft Word Tips for Your Business with SWK

SWK Technologies can provide your users with more Word tips, as well as additional education and support for getting the most out of Microsoft 365 and Office 365. Take advantage of our Managed Cloud Services to develop, hosted and cybersecure your Windows apps and ensure that you capture the best value from your implementation.

Contact us here to learn more Microsoft tips and receive real-time support for your Office suite.