Monthly Cybersecurity Newsletter

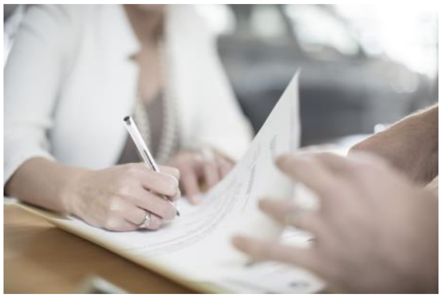
August 2021 Issue

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the Interim State Chief Risk Officer – Rob Main

Including Security and Data Privacy Terms in Contracts



The state of North Carolina is increasingly relying on Software as a Service (SaaS) vendors to provide services and solutions.

One challenge in procuring cloud-hosted solutions is ensuring that vendors will provide sufficient security controls to protect state data that will be hosted in these environments. Agency staff are often under pressure to negotiate an increasing volume of SaaS contracts quickly to meet a specific need, schedule or funding requirement, while often limiting the attention given to negotiating key security terms. Many times, security groups are brought in much later or included as an afterthought once a vendor solution has *already been selected*.

More and more, state services and solutions are being procured from cloud-hosted vendors. Shifting to a cloud environment, however, does not absolve the state of risk and responsibility. It is imperative that state organziations ensure certain requirements are set and met within contracts to meet security compliance.

Many SaaS providers represent key terms in their contracts as non-negotiable. This means that too many SaaS contracts are being signed “as is,” leading to unbudgeted costs and non-compliance to state requirements throughout the contract term and at renewal. In a recent Gartner survey, 43% of respondents answered that SaaS deals were difficult to negotiate. Compare this to only 29% stating that on-premises software was difficult. Unfortunately, data security and privacy cannot be governed *exclusively* through a contract. Although the provider is responsible for providing security of the data, the data/business owner is accountable if adequate security is not provided.

It is imperative that business owners and statekeholders investigate all security requirements ***before*** they select a SaaS vendor. For example, if the provider does not currently have an independent certification the attests to the ability of the vendor to provide adequate security controls, then do not expect the vendor to provide acceptable security for your business. Gartner recommends that a SaaS provider complete a third-party attestation, such as a Service Organization Control (SOC) Type 2 audit report or the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001 and 27002 assessment. These are two third-party attestations that the state of North Carolina also accepts.

It is also imperative to ensure data privacy terms are suitable. Most large providers have a standard data processing addendum, and you will probably need to review it. However, some providers might not meet all the state's privacy requirements. For example, a SaaS provider might not be able to guarantee that state data will be stored or processed within the continental United States, which is a ***requirement*** for solutions hosting state data. Be sure to include data security and privacy policies in exhibits to the contract, and refer to those exhibits in the relevant contract clauses.

When soliciting bids for cloud hosted solutions, be sure the vendors provide a completed Vendor Readiness Assessment Report (VRAR). The VRAR can aid an organizaton in determining whether a vendor can meet certain state security requirements and can assist agencies in vetting potential vendors. In addition, the state requires that SaaS providers that will host restricted or highly restricted data provide a third-party attestation ***annually***. Vendors that cannot meet this requirement should be rejected. State agencies should also include in their contracts the explicit right to terminate the contract should an approved third-party attestation report reveal severe risks or show that risks are not mitigated within a reasonable time.

Be sure to check out the on-demand webinar from KnowBe4 on Addressing the Challenge of Third-Party Vendor Risk that is mentioned in this newsletter.

84% of Organizations Experienced Ransomware and Phishing-Related Security Events in the Last 12 Months

New research from Trend Micro and Osterman Research highlights where organizations are strongest and weakest at stopping phishing attacks resulting in ransomware. Research indicates that ransomware is a two-pronged problem. Part of the problem is the prevalence and ease of access to very sophisticated ransomware technology. The other part of the problem is how well organizations can stop attacks. Only 16% of organizations reported no security incident types related to phishing and ransomware in the past 12 months. In other words, it is a widespread problem for most organizations.

New data in Trend Micro's How to Reduce the Risk of Phishing and Ransomware report exposes where organizations are struggling to stop attacks. Despite the efforts of many organizations to protect themselves against phishing and ransomware threats, the report indicates the percentage of organizations that have experienced 17 different types of security incidents. The top three are:

- A business email compromise (BEC) attack was successful in tricking at least one lower-level employee within the company (53% of organizations)
- A phishing message resulted in a malware infection (49%)
- A phishing message resulted in an account compromise (47%)

The report stated that among the most effective mitigations against phishing attacks and ransomware are multi-factor authentication and *security awareness training*. While the report indicates that security awareness training is part of an effective strategy to counter phishing and ransomware threats, it is unclear whether the "training" that is provided to users in most organziations is truly effective. Many organizations classify annually breakroom training or monthly email reminders as "awareness training". Individuals, however, need to be constantly updated on the latest phishing campaigns, attack methods, social engineering tactics and their personal responsibility in the organization to reduce the risk of a cybersecurity incident.

KnowBe4, a cybersecurity training and awareness vendor, claims that the combination of ongoing training modules and frequent phishing simuations can reduce the 30%+ of employees failing a phishing test down to just 4.7% of employees – a reduction in the human threat surface of 87%.

Register for the 2021 N.C. Digital Government Summit

The North Carolina Digital Government Summit is virtual again this year, and registration is now open. The virtual summit is scheduled for August 31 from 8:30 a.m. to 3:30 p.m. Gov. Roy Cooper and Secretary Jim Weaver will offer opening remarks. You'll also hear from industry thought leaders including our NCDIT colleagues.

Raju Gadiraju, Chief Information Officer (CIO) for the N.C. Department of Commerce, Division of Employment Security will be co-leading a session on preparing IT infrastructure for the next disaster. Interim State Chief Risk Officer Rob Main will be a panelist for a session about the changing threat landscape now that more people are working remotely. State Solutions Director Glenn Poplawski will be talking about digitizing government services. More speakers will be announced.

Topics for the summit include digital equity, cybersecurity, data sharing and cloud strategies. To view the full agenda and to sign up, visit https://events.govtech.com/North-Carolina-Virtual-Digital-Government-Summit.html.

KnowBe4
Human error. Conquered.

ON-DEMAND WEBINAR

Addressing the Challenge of Third-Party Vendor Risk: Securing Your Supply Chain

Your customer data, intellectual property and financials are the lifeblood of your organization. If lost or leaked, there could be significant implications to the viability of your organization. Maintaining control of that data, especially with third-party services, can be extremely challenging and requires that you ask the right questions and enforce stringent security policies.

In an environment of increased outsourcing, cloud computing adoption and regulatory requirements, how do you manage vendor risk and ensure you have a consistent evaluation life cycle?

In this on-demand webinar, James McQuiggan, KnowBe4's Security Awareness Advocate, will show you actionable steps you can use now to better manage your third-party vendor risk. Earn CPE credit for attending while you learn:

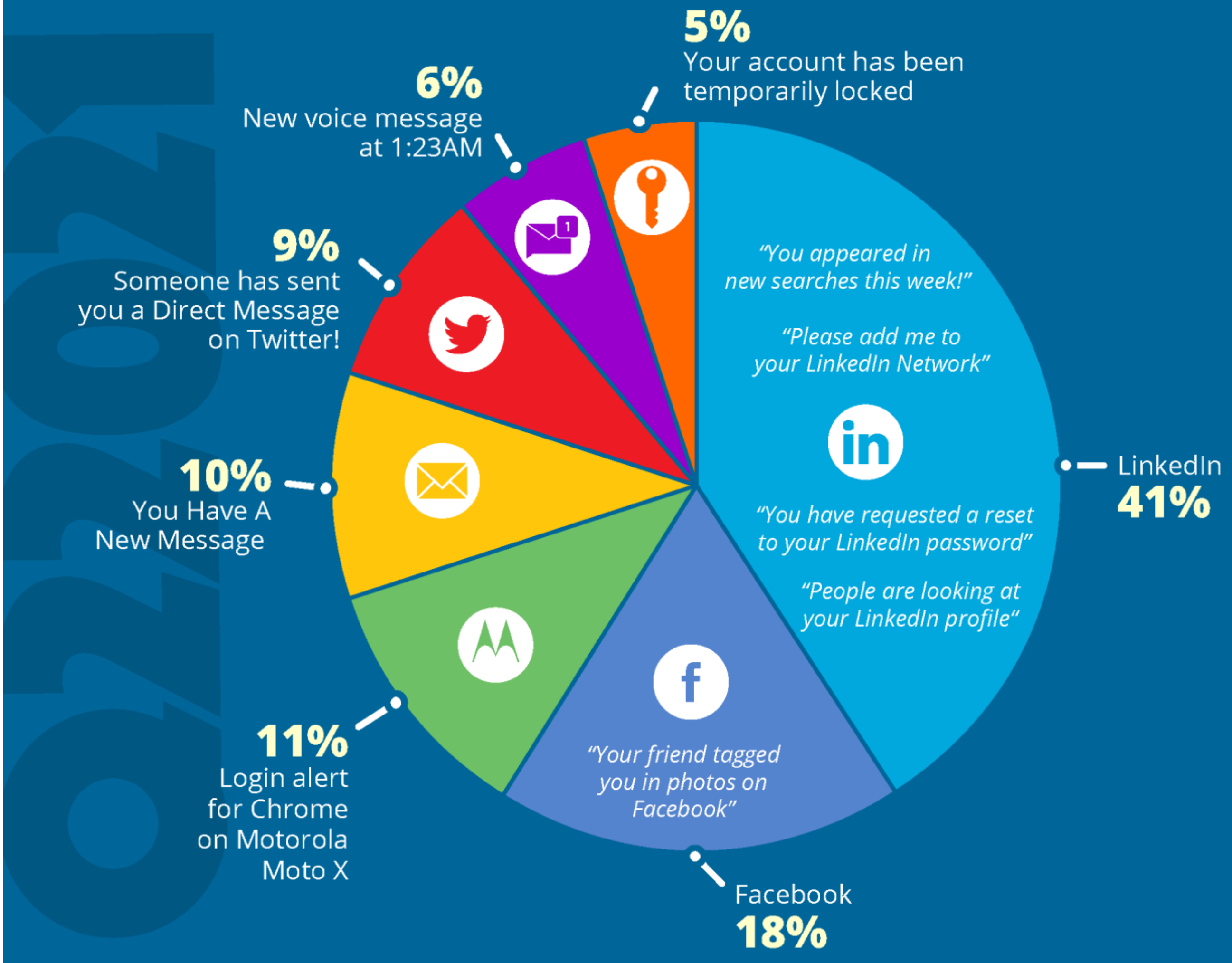
- The importance of securing your organization's critical data
- How to determine Supplier Security Proficiency
- The impact Vendor Questionnaires have on your Security Posture
- How leveraging a GRC platform can ease the burden of risk assessments and audits

Click [here](#) for more information and to register for the webinar.

KnowBe4
Human error. Conquered.

TOP-CLICKED PHISHING TESTS

TOP SOCIAL MEDIA EMAIL SUBJECTS



KEY TAKEAWAY

LinkedIn messages continue to dominate the top social media email subjects, with several variations of messages such as "people are looking at your profile" or "add me." Other alerts containing security-related warnings come unexpectedly and can cause feelings of alarm. Messages such as a friend tagged you in a photo or you have a new message can make someone feel special and entice them to click.

Microsoft Continues to Be the Top Impersonated Brand in Phishing Attacks

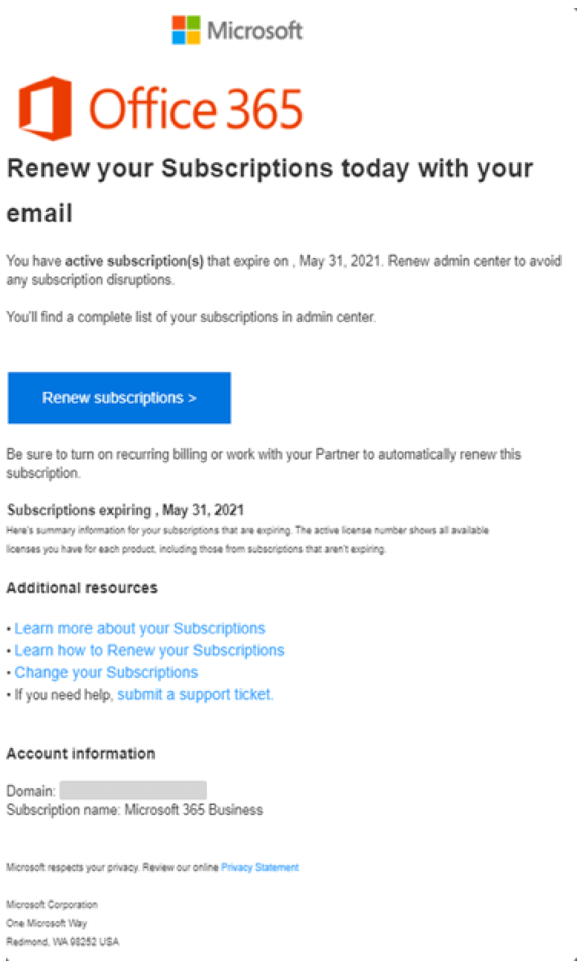
A new report from CheckPoint, a provider of IT security products – including network security, endpoint security and cloud security – identifies the leading brands that are being used by threat actors to trick victims into opening malicious attachments, clicking links, providing credentials and giving up personal details. The use of a familiar brand has been a tactic used by cybercriminals for a long time in an effort to elevate the credibility of an email, to lower the defenses of the potential victim, and to get a person to respond to a phishing email.

According to CheckPoint's Brand Phishing Report Q2 2021 blog, Microsoft is the predominate brand used in phishing attacks. The following are the top five (5) brands mentioned in the report:

- Microsoft (45%)
- DHL (26%)
- Amazon (11%)
- Best Buy (4%)
- Google (3%)

In addition, cybercriminals are getting pretty good at crafting realistic-looking emails that feel like they are really from the brands they claim. The sample image to the right, provided by CheckPoint, is one example of a phishing message that looks like the real thing.

Note how the message seems to have a look and feel that you might expect from Microsoft and could be misconstrued as being legitimate. Your only real defense is to raise the level of vigilance – the red flags should be going up first because this kind of email is ***unexpected*** and then the email's contents should be scrutinized (e.g., the email's subject reads "Your Subscription Has Been Expired" which seem a bit odd).



Renew your Subscriptions today with your email

You have **active subscription(s)** that expire on , May 31, 2021. Renew admin center to avoid any subscription disruptions.

You'll find a complete list of your subscriptions in admin center.

Be sure to turn on recurring billing or work with your Partner to automatically renew this subscription.

Subscriptions expiring , May 31, 2021

Here's summary information for your subscriptions that are expiring. The active license number shows all available licenses you have for each product, including those from subscriptions that aren't expiring.

Additional resources

- Learn more about your Subscriptions
- Learn how to Renew your Subscriptions
- Change your Subscriptions
- If you need help, submit a support ticket.

Account information

Domain: [redacted]
Subscription name: Microsoft 365 Business

Microsoft respects your privacy. Review our online Privacy Statement

Microsoft Corporation
One Microsoft Way
Redmond, WA 98252 USA

By being aware of these kinds of threats and stopping to think before you click, can reduce the risk of falling for suspicious or unexpected emails, regardless of what brand is used. For more information about phishing and how to avoid it, review NCDIT's Avoiding Phishing Attacks page.

Training and Continued Learning Resources

- FedVTE: Free Online Training Environment
  - https://fedvte.usalearning.gov/
- TEEX: Texas Engineering Extension Service
  - https://teex.org/
- NICCS: National Initiative for Cybersecurity Careers & Studies
  - https://niccs.cisa.gov/
- ICS-CERT Training
  - https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

CYBERSECURITY NEWSLETTERS

SAC Security Awareness Newsletter: Monthly security awareness newsletter provided for all state employees by KnowBe4.
***Note**: You must have a valid state employee O365 account.*

- https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/Security%20Awareness%20News/2021

CIS Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security (CIS). https://www.cisecurity.org/resources/?type=newsletter

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by the SANS Institute. https://www.sans.org/newsletters/ouch/

August 10: SANS Webinar: Securely Transitioning Workloads to the Cloud

August 11: SANS Webinar: How does your incident response program stack up?

August 31: North Carolina Digital Government Summit

October 5-6: 2021 N.C. Cybersecurity Awareness Symposium

October 18-22: Cyberweek

Also, for a list of upcoming SANS webcasts, visit here.

Be sure to follow the N.C. Department of Information Technology on Twitter, Facebook and LinkedIn for more tips. Also visit it.nc.gov/CyberSecureNC or Stay Safe Online for additional information and resources on cybersecurity awareness. *Remember… Stop. Think. Connect.*

***Disclaimer**: Vendors, references, and links in this newsletter are for informational purposes only and their inclusion should, in no way, be considered an endorsement from the N.C. Department of Information Technology.*