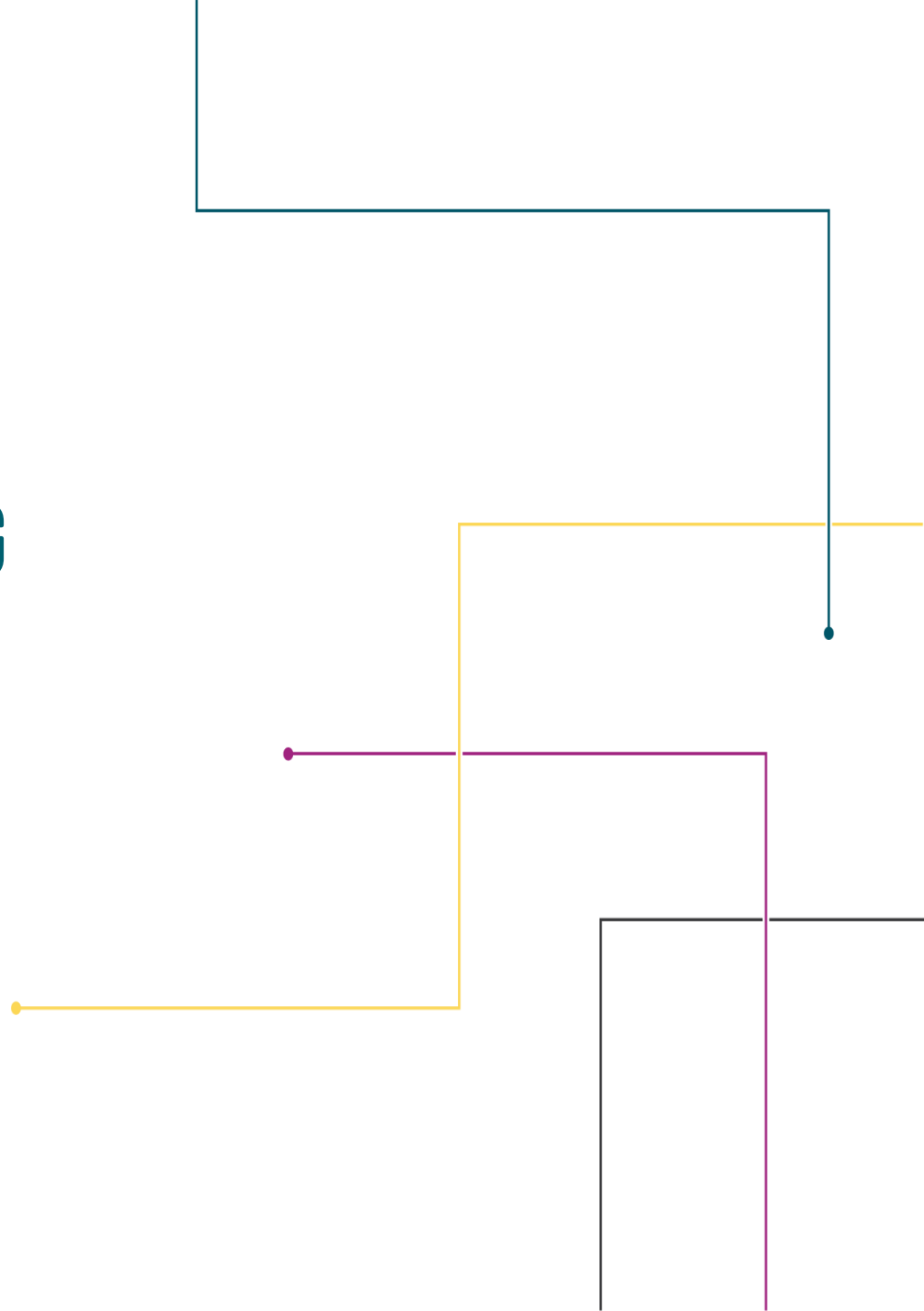




# ISOAG MEETING

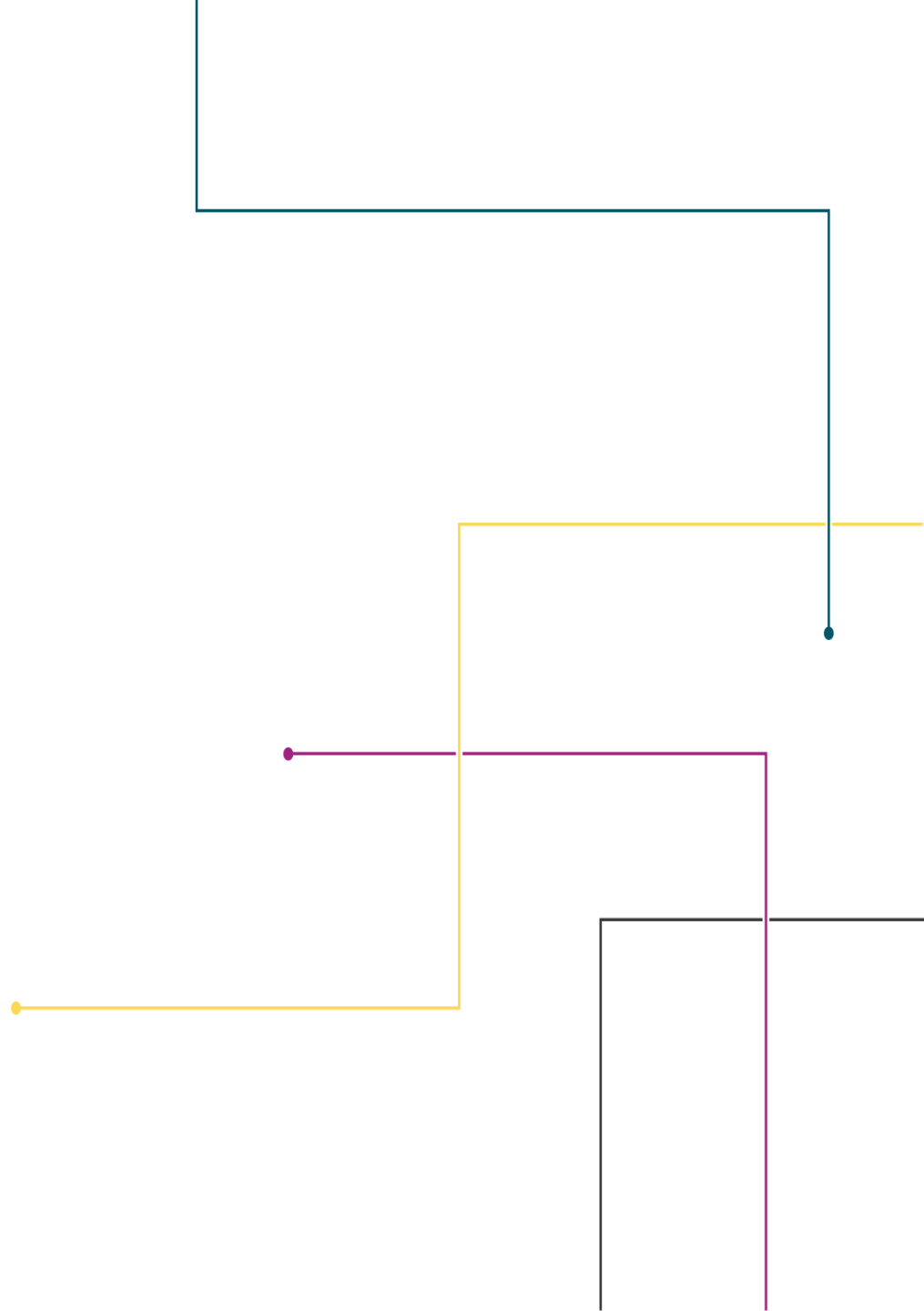
## JAN. 6





## AGENDA

- **BRYAN CARNAHAN, ASSURA**
- **DAN HAN, VCU**
- **JON FORD, FIRE EYE**
- **TINA HARRIS GAINES, VITA**





A S S U R A I N C

ISOAG

After Action Review of a Ransomware  
Incident

January 6, 2021

# Assura, Inc.

- Formed in 2007 & Headquartered in Richmond, VA
- Dynamic services firm focused on:
  - Cybersecurity and Information Protection
  - Business Continuity
  - Assurance and Compliance
- Core services:
  - Cybersecurity GRC
  - Managed services
  - Testing & evaluation
  - Engineering
  - Incident Response
  - Audit



## **Bryan Carnahan, CISM, Security+**

- Client Success Manager of our Governance, Risk, and Compliance Department
- Background in developing Policies and Procedures, Incident Response, and IT Disaster Recovery Plans
- 5 years of experience providing information security services to state agencies and the private sector.

# Talking Points

**1** Ransomware and Why?

**2** Incident Background

**3** Compromise

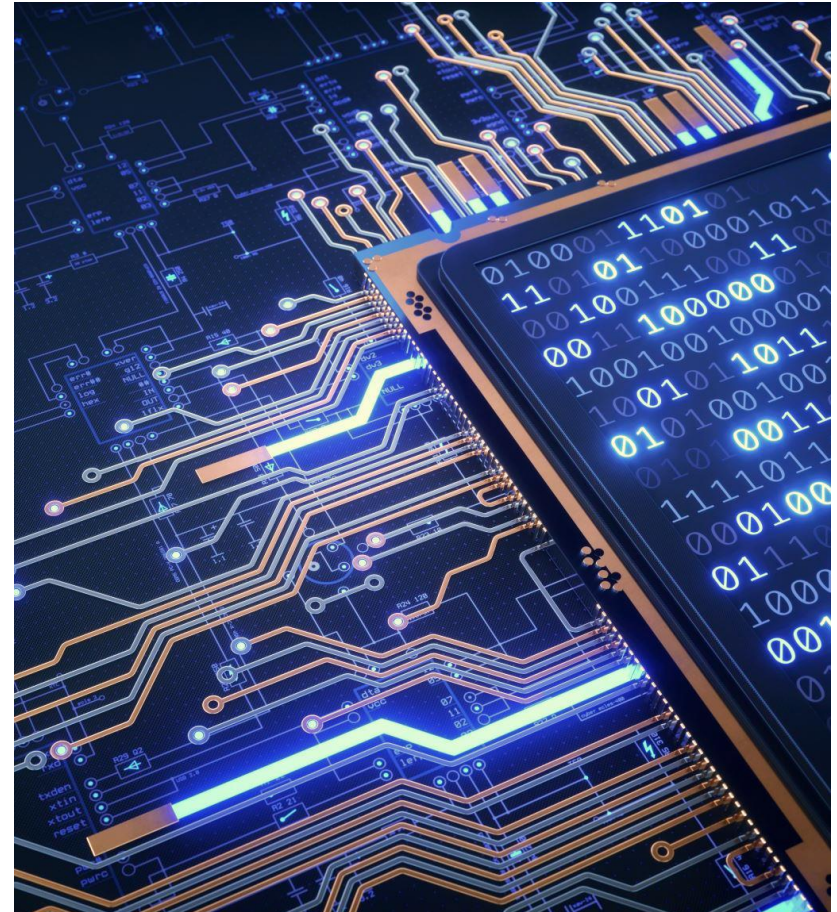
**4** Response

**5** Recovery

**6** Resolution and Questions

# Ransomware – What is it?

- We are all familiar with the concept; A piece of malware that encrypts your data and locks access behind a paywall
- Boogeyman of our industry
- Although it is pervasive, few have had the opportunity to experience or to respond to a ransomware incident  
(Thankfully)



# How do we train effectively against something so uncommon?



- Best method is to simulate an incident and perform an exercise fooling a well-developed IR Plan.
- Today we'll go over a recent ransomware incident that Assura provided Incident Response for
- Cover Compromise, Containment, and Recovery
- Identify security controls that can improve your defense to cyber attacks

# Defining Our Characters

Going to be using general terms to protect the innocent:

- **Company** refers to business who experienced the Ransomware incident
- **Service Provider** refers to Company's primary IT Infrastructure and Support vendor
- **Vendor** is responsible for performing an asset inventory for the Company
- **Forensics** is a team brought in to identify source of compromise







# Background

- January 9<sup>th</sup>, 2020
- Private Sector Company with multiple locations
- Relies on Service Provider for infrastructure and onsite support
- Company's IT is managed through a central office, with less than 5 staff members



## Background (cont.)

- Company's previous IT Director retired at the end of the previous year
- New IT Director has been hired to fill the position
- First action is to perform an asset inventory
- Discovers widespread End-of-Life (EOL) OS and Software use



## Background (cont.)

- IT Director hires a Vendor to assess assets at each location
- Vendor will run an application on each device, transfers via USB
- Vendor needs an Admin account
- Vendor delivers a list of which assets are running EOL OS and software

# Compromised Vendor

- The vendor had been compromised for quite a while
  - Vendors who provide IT services are often targets
  - Compromise one, get access to their whole client base (Supply Chain Attack).
- Malware spread from the vendor's equipment to Company's assets
  - The Company's regular virus scans did not identify the malware
  - Moved through the network using provided admin credentials

# Compromise – What Went Wrong?

## Your environment, your equipment.

- If you're going to have someone performing a task within your environment, provide them with equipment that you trust for use
- Application could have been independently downloaded, scanned, then distributed when determined to be safe
- Don't cave to vendor's frustration



# Compromise – What Went Wrong?

## Patch Management and Updates

- Many AV tools can only catch what they know to look out for
- Updates may be automatic but could depend on regular restarts
- It only takes one device to be compromised



# Compromise – What Went Wrong?

## Excessive Privilege

- Privileged accounts should be distributed out rarely
- Account was not disabled immediately post vendor use.
- Account could have been set to automatically expire and avoid human error.



# Response - Timeline

Time	Action
5:27 AM	Service Provider identifies issue
5:30 AM	Service Provider reaches out via email and cell phone. Does not get a response
6:30 AM	IT Director returns call
6:35 AM	IT Director attempts to log in remotely, is unsuccessful
7:45 AM	IT Director arrives onsite and is able to login via local credentials onto one of the servers. Internet Explorer automatically opens when they login
<b>Greeted with the following message</b>	



# Internet Explorer Note

**Contact required for further action:**

**kellsbells@protonmail.com**

**allymitch@protonmail.com**

**Balance of Shadow Universe**

**RYUK**

# Response – Timeline (cont.)

First moment that the IT Director is aware that they've been compromised

Time	Action
8:00 AM	Contacts Service Provider, requests support
8-8:30 AM	Users begin to try to login, are having issues
8:30 AM	Company reaches out to Assura for additional support
9:00 AM	Service Provider and Assura begin incident response
10:00 AM	Leadership is notified
10:05 AM	CFO activates cyber insurance policy.

# Response – What Went Wrong?

## Insufficient Monitoring and Response

- First identifying an issue from when it successfully disrupts a service is not effective
- Monitoring should include logs from devices and alert staff to unusual activity
- Example alarm: Multiple administrative logins outside of 8 AM – 5 PM
- Intrusion Detection and Prevention Systems (IDS and IPS)



# Response – What Went Wrong?

## **Lack of Backup Communication**

- A single method of communication is a single point of failure
- While Company had phones and email, they were both managed by one entity
- Have multiple forms of communication and train staff on how to use them when necessary



# Response – What Went Wrong?

## Notifying Leadership

- Leadership didn't find out about the scale of the incident for two hours post discovery
- Leadership's primary role is to make and communicate decisions throughout the organization
- Had the new IT Director notified leadership, the CFO would have quickly been able to activate Company's cyber insurance policy





# Recovery

- After a few hours, Service Provider, Forensics and Assura can ensure full containment and eradication of malware
- Devices that were affected are still encrypted
- Forensics requires a few hours to create images for investigation purposes
- Assura works with Service Provider to attempt recovery of backups



## Recovery (cont.)

- Backups are non-functional
- Previous IT Director had a 'set it and forget it' approach
- Discussion with leadership leads to communication with attackers and paying ransom for mission essential systems
- Total cost for this small company was \$226,000 in bitcoin. After negotiations



# Recovery – What Went Wrong?

## Untested Backups

- Backups are a solution, but only if they work
- Regularly check your backups to ensure they are functioning
- SEC501 says 30 days, decide what works for your environment and systems





# Recovery – What Went Wrong?

## Having to Pay for Recovery

- Paying the ransom is always an option
- In the past, would have been my recommendation if you needed access to your data
- Is now illegal as of October 2020
- Weigh the costs and benefits, communicate with VITA





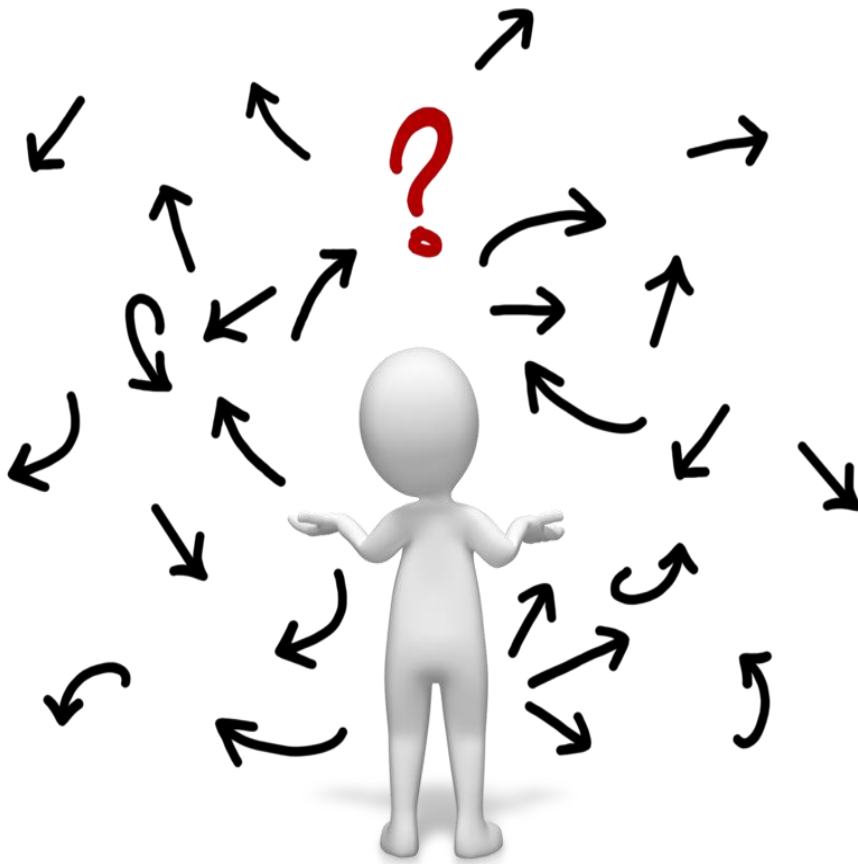
# Resolution

- Company now has 24/7/365 monitoring
- Company has developed and trained on an Incident Response Plan
- Company has ensured that backups are occurring and are tested regularly
- Company now has a target on their back – they've shown they are willing to pay

# Lessons Learned



- Your Environment, Your Equipment
- Regularly Patch and Update
- Beware Excessive Privilege
- Monitor for Attacks
- Have Multiple, Independent Communication Channels
- Notify Leadership ASAP
- Best Practices for Backups



**Contact Information**

Bryan Carnahan

[bryan.carnahan@assurainc.com](mailto:bryan.carnahan@assurainc.com)

804-767-5040

LinkedIn

# 2021 and Beyond: Information Security for the Post-Pandemic world

Dan Han

Virginia Commonwealth University

Welcome and happy new year!

# The past year has been tough...

- The COVID-19 Pandemic
- Social unrest
- Mass unemployment
- Drastic changes to how we work and interact with one another



However...



# From the odd...



This restaurant in Maryland intends to use bumper tables to keep customers six feet apart once it begins to take seated diners.



Katy Lee  
@kjalee



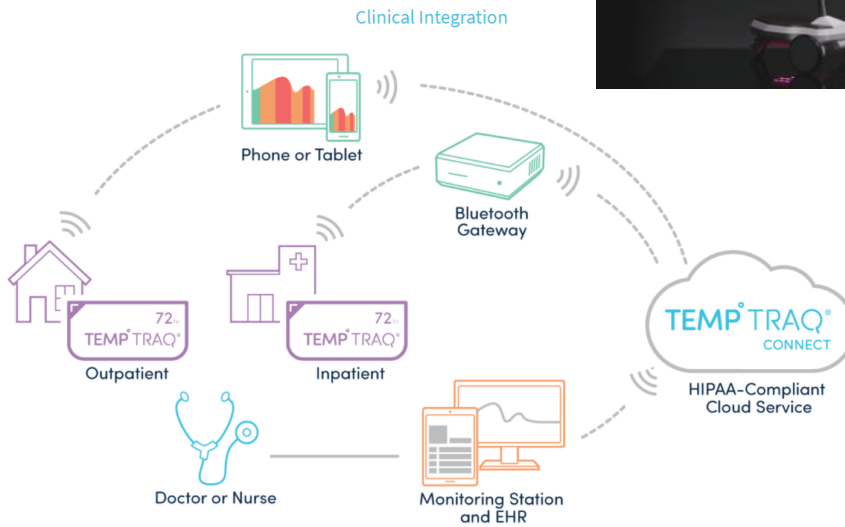
Oh my god, this is amazing. A German cafe is making people wear swimming pool noodles as hats to enforce social distancing.

Pic via Cafe & Konditorei Rothe on Facebook

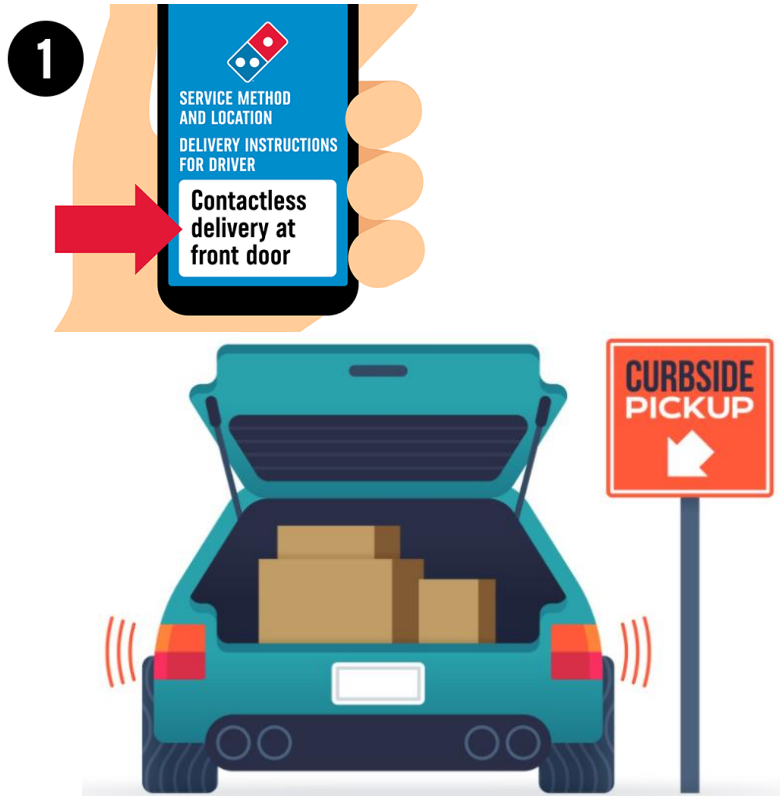
[facebook.com/30253790311707...](https://facebook.com/30253790311707...)



# To futuristic



# COVID19 = Fuel for Innovation





So what about technology and information  
security of the future?

The current demand that drove much of the changes is largely driven by the low appetite for risks related to employee and public health

# The demands of the workforce

- Aside from training and career development opportunities, a majority of Millennial and Gen Z workers preferred flexible option to remote work after the pandemic.
- **Work Whenever, from Wherever, on Whatever device I choose.**



Source: Deloitte Global Millennial Survey 2020

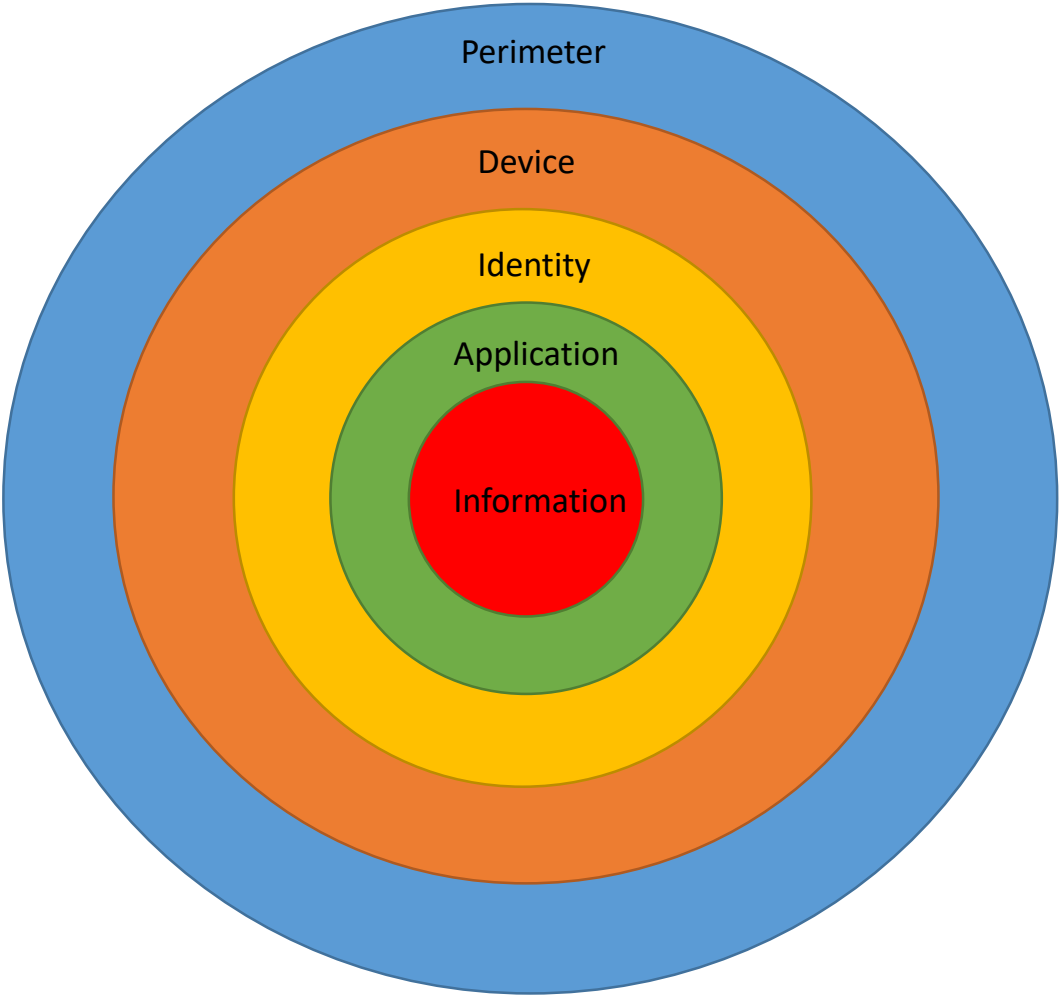
In a way, the pandemic served as a live social experiment for many organizations on the idea of remote work, and many organizations have rapidly implemented changes and found positive results from it



# Let's take a look at some of these changes

- Work From Home
  - Organization issued computers or BYOD
  - Provisioning of Internet Access
  - Remote access to internal systems
  - Telephone
- Remote Services
  - Scalable services to meet the demands
  - Ability to schedule in-person visits
  - Virtualization of in-person services
- Density monitoring and Contact Tracing
  - Use of wireless technology

From an Information Security Perspective...



# Work from Home

- The option to work-from-home may be here to stay
- Current model may include the use of VPN, an organization assigned workstation or BYOD
- Leverage of teleconferencing and chat software
- Traditional perimeter based defenses may not be as effective



# Work From Home and Short-term mitigations

- Efficacy of on-prem security controls have been decreasing over the years, the pandemic only accelerated it.
- Pieces of the Zero Trust model and Software Defined model may be or may have been used for a new security architecture.
- Additional targeted deployment may help with visibility and risk mitigation

# Short-term controls – Endpoint (Device layer)

- EDR platform or endpoint monitoring
  - Enterprise EDR platforms such as CrowdStrike, Cybereason, MS ATP, etc can be deployed to all or high risk units to help augment monitoring of endpoints regardless of their location.
- The cheaper alternative/supplement
  - For those of us who may not have funds to cover the workstations:
    - Sysmon / Powershell Block, Module, Module Name logging
    - Use XPATH query to configure logs and forward events back to a collector
    - A good sysmon config file starting point: <https://github.com/SwiftOnSecurity/sysmon-config>

# Powershell logging

- Need the following registry entries:
  - HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging::EnableScriptBlockLogging::1::Dword
  - HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging::EnableModuleLogging::1::Dword
  - HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging\ModuleNames::\*::\*::String
- Logs will show under *Application and Service Logs > Microsoft > Windows > Powershell > Operational*

# Sysmon configuration

- Sysmon by default is very noisy
- You need to fine tune sysmon with a config XML file for your environment
- A great starting point is the sample config file created by SwiftOnSecurity at: <https://github.com/SwiftOnSecurity/sysmon-config>
- Sysmon logs can be found at *Application and Service Logs > Microsoft > Windows > Sysmon > Operational*



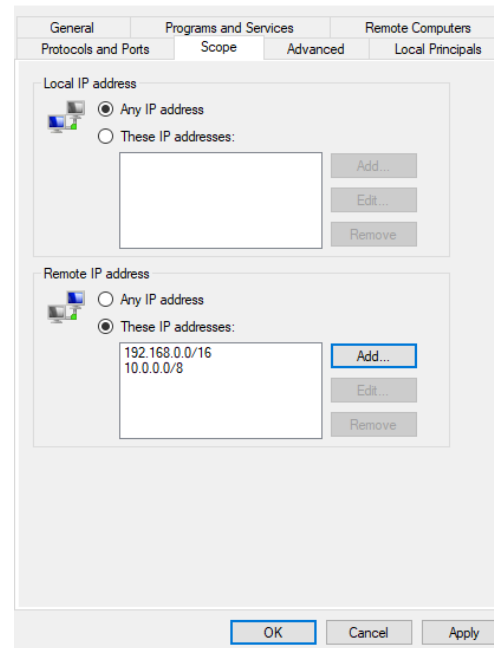
# Windows log forwarding

The following is a sample XPATH query to use with event forwarding for System, Application, Security logs (minus info level items), as well as Powershell and Sysmon logs...

```
<QueryList>
  <Query Id="0" Path="Application">
    <Select Path="Application">*[System[(Level=1 or Level=2 or Level=3 or Level=5)]]</Select>
    <Select Path="Security">*[System[(Level=1 or Level=2 or Level=3 or Level=5)]]</Select>
    <Select Path="System">*[System[(Level=1 or Level=2 or Level=3 or Level=5)]]</Select>
    <Select Path="Microsoft-Windows-PowerShell/Operational">*[System[(Level=1 or Level=2 or Level=3 or Level=5)]]</Select>
    <Select Path="Microsoft-Windows-Sysmon/Operational">*</Select>
  </Query>
</QueryList>
```

# Short-term controls - Endpoint

- Windows Firewall
  - Enforce firewall rules through GPO
  - In addition to the default blocking of typical ingress traffic
  - Block egress access to RDP and SMB with the exception of approved server ranges.



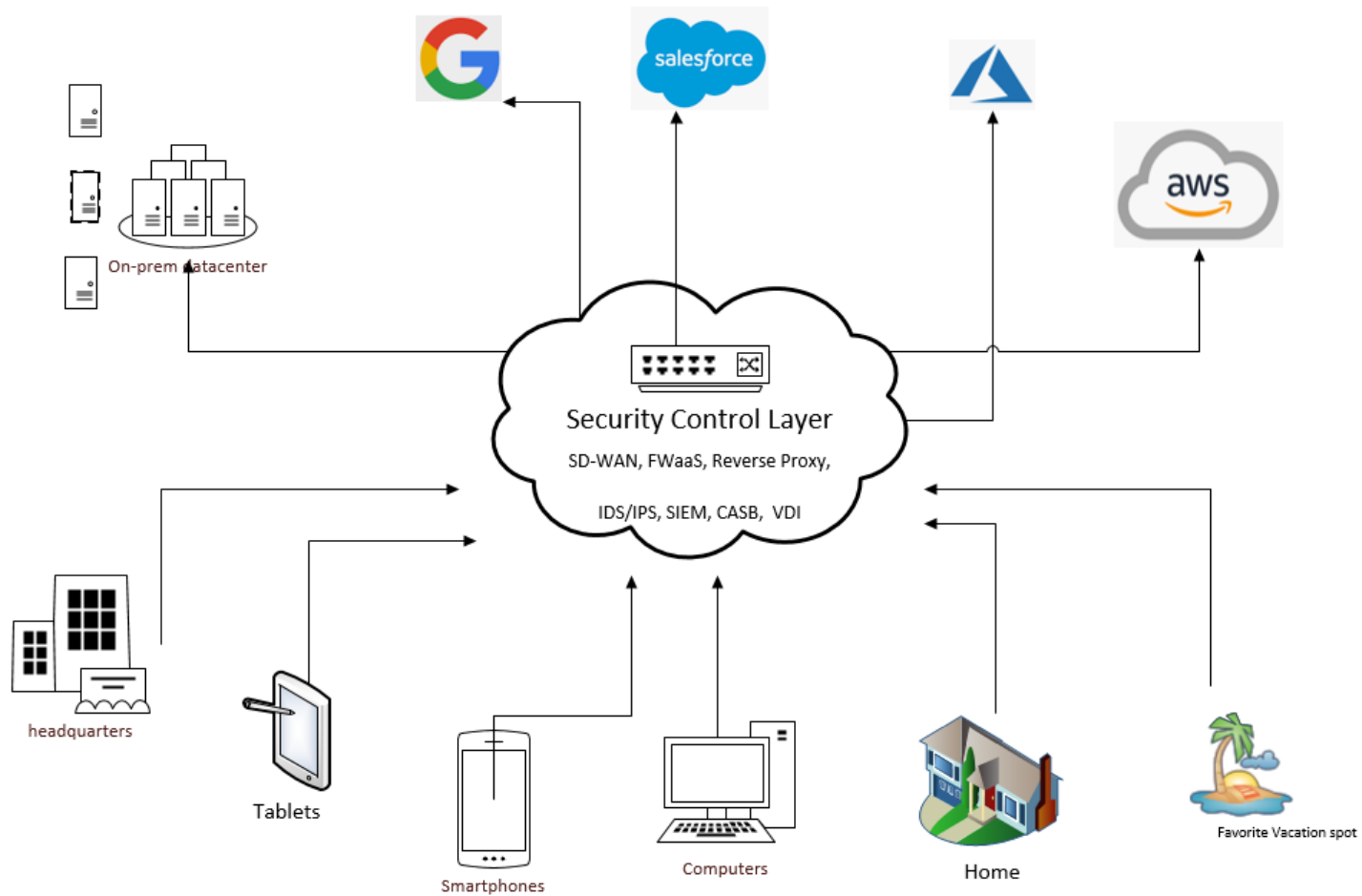
What about BYOD?

# Short-term controls - Identity

- Authentication Control and Logging
  - Strong passwords and Multi-factor authentication enabled single-sign-on should be deployed systems
  - Authentication logs must be collected and analyzed
- Behavioral analysis
  - Device, location, and browser analysis and continual monitoring
  - Long term: ML models of expected behavior and actions taken upon anomaly
- Device health check
  - Perform basic health checks of devices upon connection, identify patch level, presence of AV, etc.

# Rethinking the security architecture of the post-pandemic world

- Shift to Secure Access Service Edge and a Software Defined Zero-Trust model
  - Separation of security control plane from the physical plane of the organizational environment
  - Goal is to issue a single set of policy for subjects and objects, regardless of their physical location or device utilization.
  - Investment into Firewall as a Service, SD-WAN, and cloud based reverse proxy tools
  - Investment into Cloud Access Security Brokers and IDS/IPS as a service.
  - For those who wants to go a step further, look into VDI-as-a-Service solutions like Azure WVD to provide compliant devices regardless of location.



Shifting gears a bit...

# Virtualization of services

- Rapid development and scaling of virtualized in-person services
- These services may need to be scalable in order to accommodate demand
- May lead to heavier shift toward cloud based and server-less architectures
- May further erode the traditional network perimeter
- Requires additional application and identity layer controls



# From an human interaction perspective

- Teleconferencing and Collaboration/Chat tools will be more accepted as normal means of communications.
- Security guidance for virtual meetings and configuration management for teleconferencing tools
  - Meeting setup and management
  - Meeting link publication
  - Storage of recordings and transcripts



# Dual-use of tracking technology and privacy

- The investments made by organizations in leveraging technology to help with contact tracing and social distancing can potentially be reused for other purposes
- Important to outline privacy policies and expectations to organizations and individuals about the reuse of this technology

# Summary

- Remember the aspiration is to provide consistent and secure services whenever, wherever, and to whichever device an individual uses
- Look for quick wins to shift monitoring and prevention to devices
- Move the focus from perimeter to identity, application, and data
- Investigate and plan to apply software defined principles to your security architecture
- Plan for expanded electronic service offerings for traditionally in-person services, and prepare to include these services in your security model
- Create and maintain guidelines and support for teleconferencing and collaboration services
- Consider privacy implications when reusing technologies for purposes outside of contact tracing and occupancy monitoring due to the pandemic

Thank you

Questions?



# A Global Reset: Cyber Security Predictions 2021

Report Insights

Jon Ford  
Managing Director  
Mandiant Solutions

# Agenda

- Frontline Threat Activity
- The Evolution of Security Validation
- State of the Cloud 2021
- Q&A
- Closing



**Jon Ford**  
Managing Director  
Mandiant



# Frontline Threat Activity

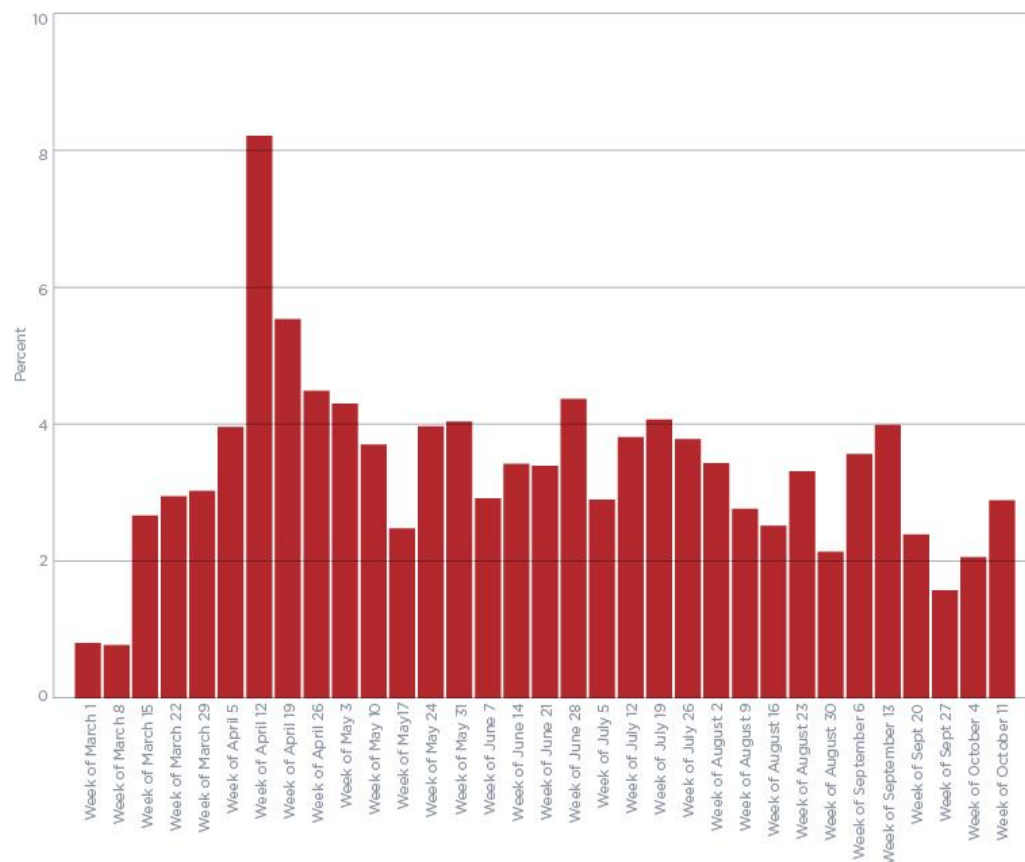


# COVID-19

- Wide range of threat actors have incorporated coronavirus-themed lures into their phishing operations.
- Instances in Europe, East Asia, and elsewhere of coordinated inauthentic campaigns and disinformation networks leveraging COVID-19.
- Increased risk to healthcare, pharmaceutical, and public health organizations.

## CORONAVIRUS-THEMED PHISHING AS % OF ALL MALICIOUS EMAIL DETECTIONS BY WEEK

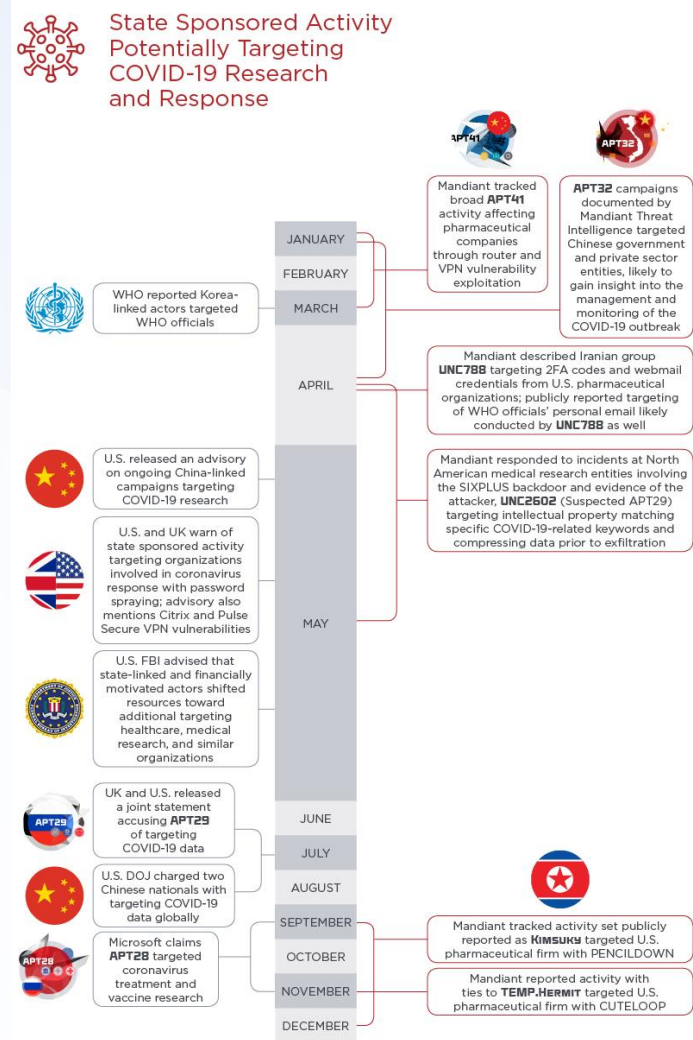
March 1 - October 17





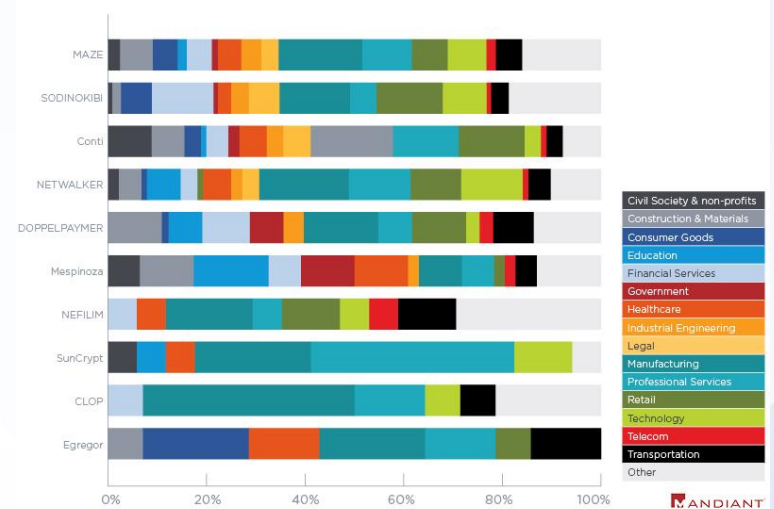
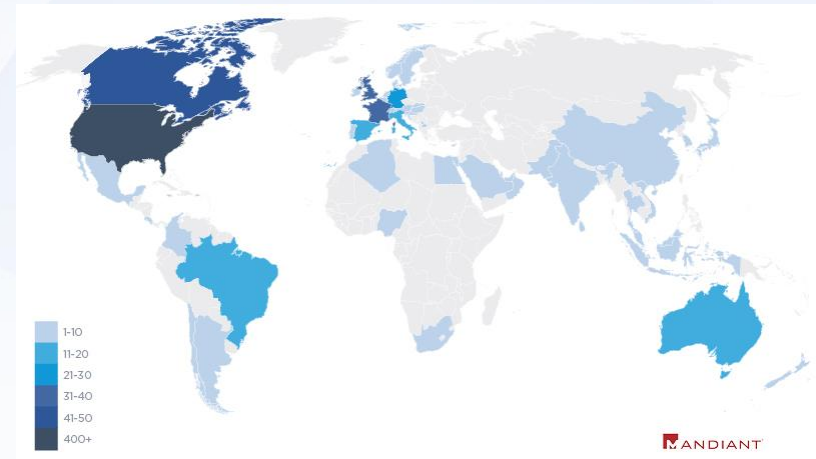
# Cyber Risks to Pharmaceuticals and Healthcare Remain Elevated Due to Coronavirus

- Throughout 2020, we have observed state-sponsored activity targeting organizations directly involved in COVID-19 treatment and response from Vietnam's APT32, China's APT41, Russia's UNC2062 (suspected APT29), Iran's UNC788, and two North Korean activity sets. We suggest that intelligence gathering is a likely motive, though there is also a risk of IP theft.
- Ransomware has continued to affect hospitals, retirement communities, and medical centers throughout the coronavirus (COVID-19) pandemic. Research laboratories working to develop vaccines and treatments have been targeted as well.



# Ransomware



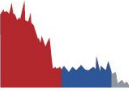



- Throughout 2020, Mandiant Threat Intelligence observed threat actors increasingly incorporate data theft into ransomware operations. In these cases, the actors exfiltrate data from victims, which they threaten to post publicly if not paid.
- We expect malicious actors will continue combining ransomware operations with data theft and extortion, as it gives threat actors additional leverage and increases their likelihood of being paid.



# Return of More Chinese APT Actors

- We have continued to observe the return of Chinese espionage groups after periods of dormancy and currently active groups engage in frequent and widespread campaigns.
- Some groups observed with increasing frequency and outside traditional geographic focus areas.
- Tempo of Chinese state-sponsored activity could increase in the future and bears watching as Chinese cyber espionage operators are more stealthy and agile than in years past.

## Chinese Cyber Espionage Evolves to Support Higher Level Missions

	2012-2015	2016-2019	
<b>Goals</b>	IP theft, competitive advantage, strategic intelligence gathering	Strategic intelligence gathering, competitive advantage	
<b>Targeting Pattern</b>	Somewhat opportunistic sector-wide targeting, inefficient, frequent targeting of high tech and other innovative sectors	More efficient and purposeful, i.e., targeting the communications backbone and organizations with access to third parties	
<b>Tempo</b>	High volume	Lower volume	
<b>TTPs</b>	Noisy, persistent, little opsec	More stealthy, agile, complex to attribute, better opsec	
<b>Actor Mix</b>	APT1, APT3	APT41, APT40, APT19, new activity sets	
<b>Geographic Distribution</b>	Focused on U.S.	Focused on Asia	

# Russia Will Likely Maintain an Aggressive Posture Throughout 2021

- Mandiant Threat Intelligence assesses with high confidence that Russian cyber espionage operations presented a sustained and serious threat to multiple industry sectors in 2020 but posed the greatest threat to governments in Russia's near abroad and NATO Member States, particularly Poland, Ukraine, and the U.S.
- We discovered a supply chain attack trojanizing SolarWinds Orion business software updates in order to distribute a backdoor we call SUNBURST. This campaign may have begun as early as spring 2020, and we track the actors conducting it as UNC2452, although media reporting has attributed this campaign to APT29 and the Russian Foreign Intelligence Service (SVR).

## DISTRIBUTION OF RUSSIAN CYBER ESPIONAGE AND INFORMATION OPERATIONS

September 2019 - October 2020



# Iranian Espionage and Information Operations May Intensify in 2021

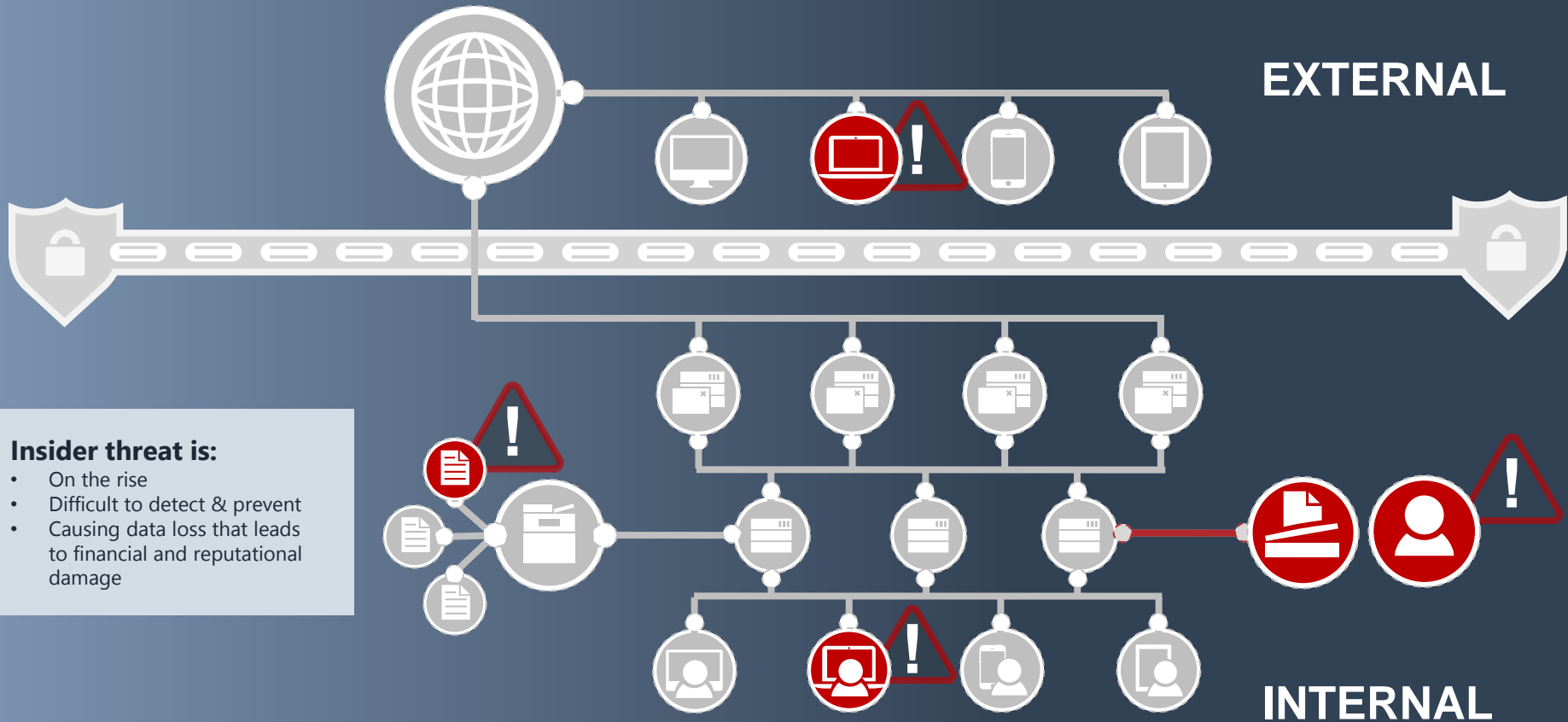
- We assess with high confidence that Iranian cyber espionage and information operations present a high-frequency and high-intensity threat to public and private sector entities globally. We suggest several factors may lead to an intensification of Iranian espionage, destructive, and information operations in 2021:
  - The economic and geopolitical situation in Iran has deteriorated throughout 2020. Financial pressure from new economic sanctions, a drop in oil prices, and a country-wide shutdown to contain the coronavirus has caused the Iranian rial value to drop to a record low against the U.S. dollar, suggesting individuals tasking Iranian cyber threat actors are operating under stress and may act unpredictably or aggressively.
  - The January 2020 death of Qasem Soleimani by a U.S. airstrike and the November 2020 assassination of Mohsen Fakhrizadeh may increase the likelihood that Iran will seek to retaliate against the U.S. and its allies' assets using destructive malware.

# North Korea Expands Targeting Scope and Frequency in 2020

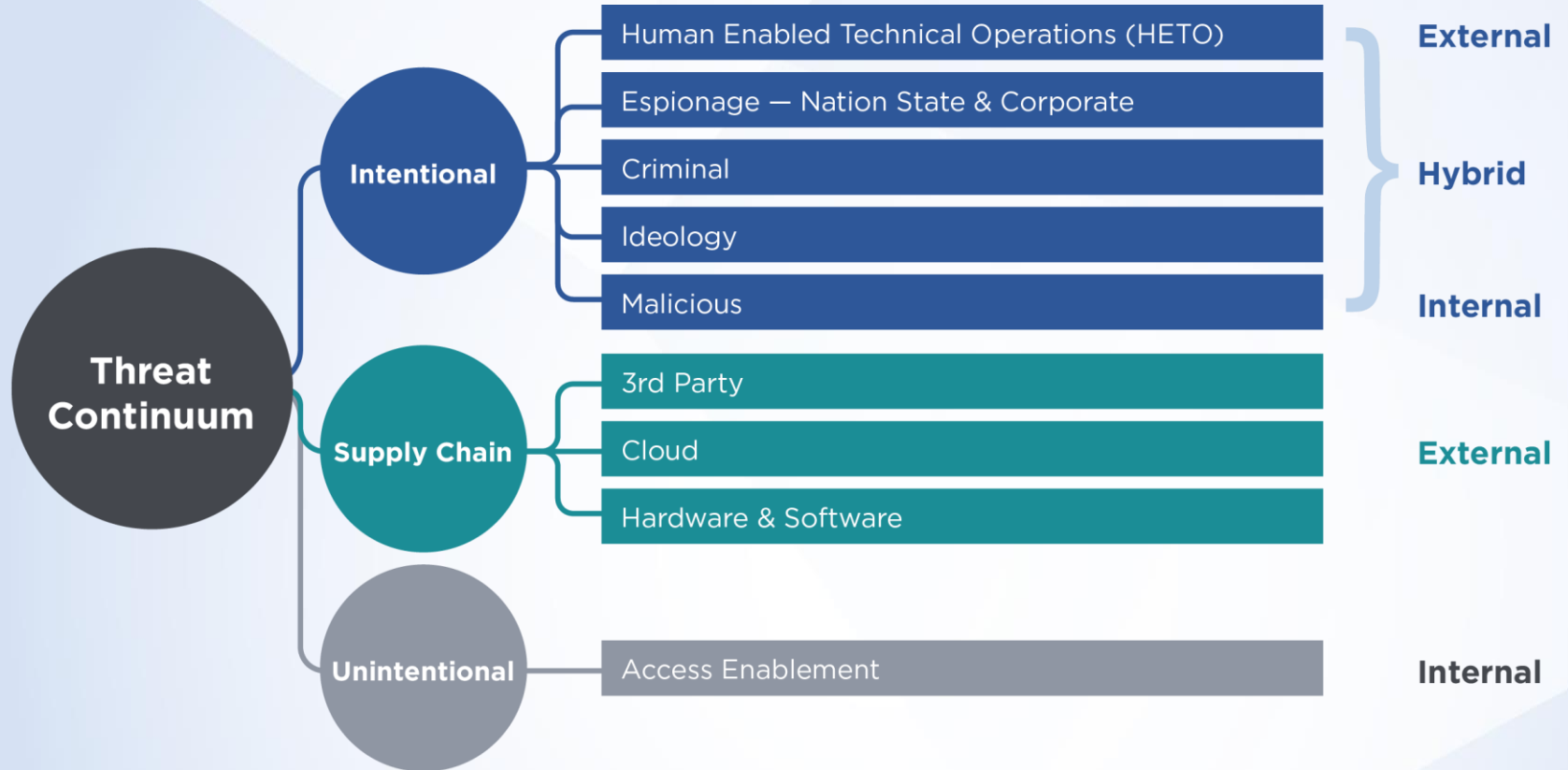
- Throughout 2020, North Korea continued to target the aerospace and defense, government, and technology verticals as well as public and private groups who have demonstrated an interest in the Korean peninsula.
- We assess with high confidence that this activity poses a frequent and moderate to severe threat globally.
- We have detected a targeting shift in North Korean espionage objectives, with state-sponsored actors expanding their scope to target the healthcare and agricultural verticals, and we have also observed an increase in the tempo of North Korean activity in late 2020.
- We suggest the frequency and intensity of espionage campaigns in 2021 will likely depend on the political climate with regard to the U.S., South Korea, and China.



# Insider Threats: A Growing Challenge



# Threat Continuum





# Motivation



EGO/REVENGE



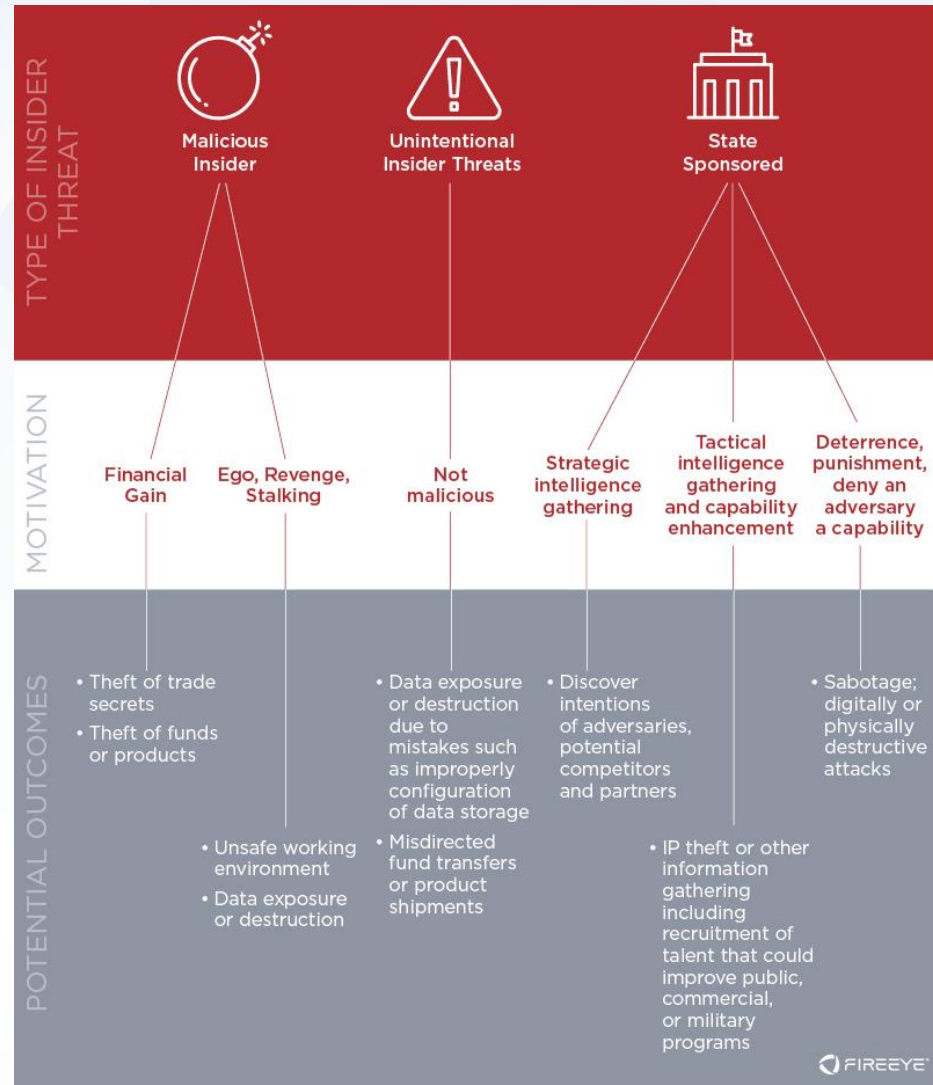
FINANCIAL GAIN



ESPIONAGE












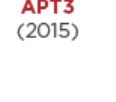









UNINTENTIONAL



# Strategic View

- Simultaneous use of insider threat recruitment and external espionage to support strategic objectives

	AUTOMOTIVE TECHNOLOGY 	ADVANCED MATERIALS 	SEMICONDUCTORS 	AVIATION AND TURBINE TECHNOLOGIES 	CANCER RESEARCH AND TREATMENT 	BIOTECHNOLOGY 
INSIDER THREATS	<b>Xiaolang Zhang</b> (2018)	<b>Xiaorong You</b> (2017 - 2018)	<b>Simon Saw-Teong Ang</b> (2018)	<b>Xiaoqing Zheng</b> (2016 - 2018)	<b>Six Moffitt Cancer Center Researchers</b> (2011 - 2019)	<b>Xiao-Jiang LI</b> (2012 - 2018)
	<b>Guangzhi Cao</b> (2018)				<b>Five MD Anderson Researchers</b> (2018 - 2019)	<b>Yu Zhou</b> (2015 - 2017)
	<b>Jizhong Chen</b> (2019)					<b>LI Chen</b> (2015 - 2018)
APT ACTIVITY	 <b>APT41</b> (2019)	 <b>APT40</b> (2017)	 <b>APT3</b> (2015)  <b>APT18</b> (2016)	 <b>APT26</b> (2010-2015)	 <b>APT18</b> (2015)	 <b>APT3</b> (2015)
		 <b>APT41</b> (2019)	 <b>APT17</b> (2016)		 <b>APT12</b> (2016)	 <b>APT26</b> (2015)
			 <b>APT20</b> (2018)		 <b>APT10</b> (2017)	 <b>APT41</b> (2018)

# What's next?

- How will IO efforts evolve, particularly in conjunction with intrusion-based campaigns?
- Continued evolutions in adversary targeting patterns due to COVID-19 and remote workforces
- Evolution of ransomware and extortion
- Continued importance of visibility of actor behavior off-network/utilization by other threat actors/ criminal – APT nexus





# The Evolution of Security Validation

# COVID & WORKING FROM HOME

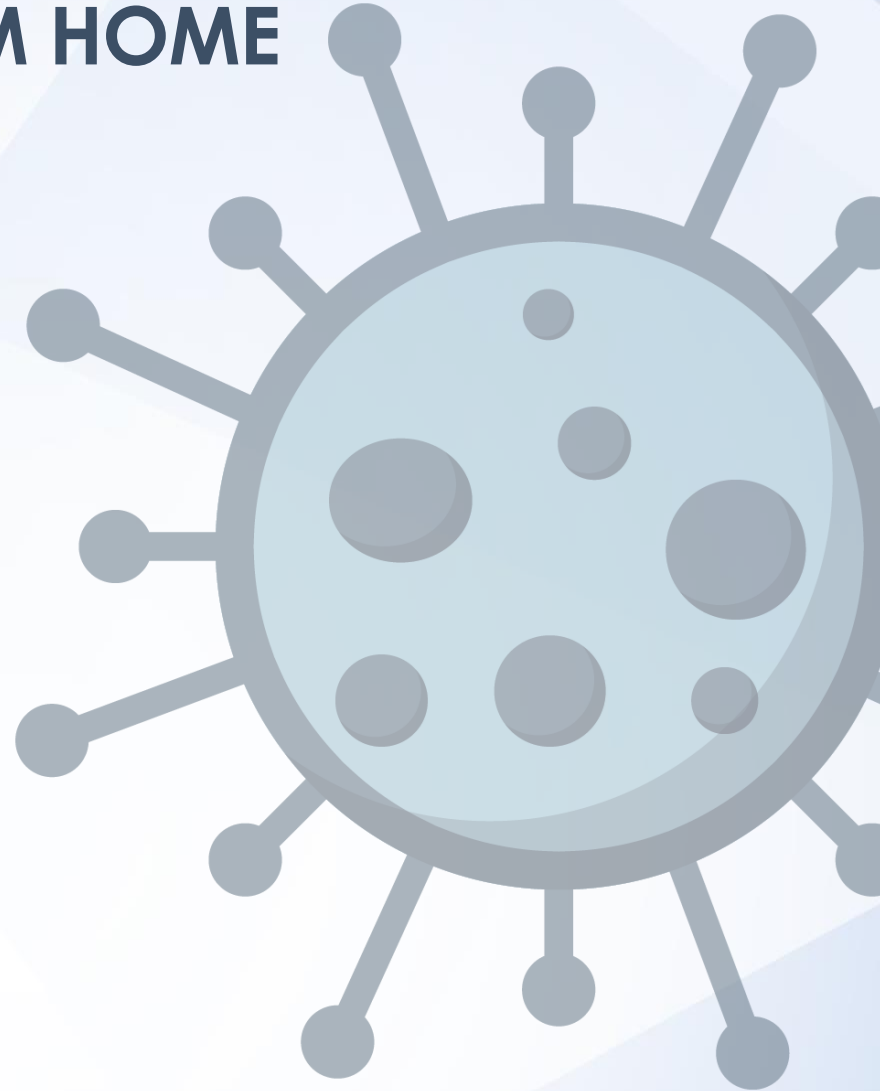
- Cloud Security



- Data Security



- Automation



# VALIDATION EVOLUTION IN 2021

- Threat Intelligence



- Incident Response



- Intelligence-Led Security



# THE BUSINESS OF SECURITY VALIDATION

- It's Not About Cyber Risk



- Leadership & Material Risk



- Strategic Security & Competency



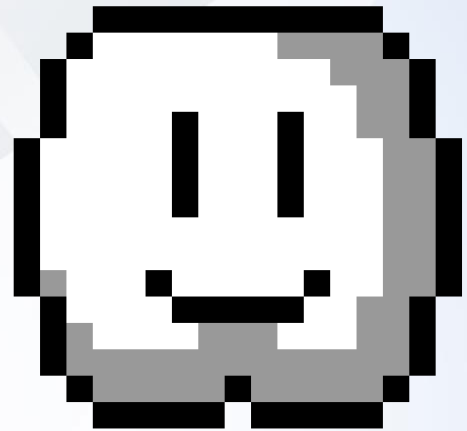
# The State of the Cloud 2021

The background is a solid teal color with several large, overlapping, semi-transparent geometric shapes in various shades of teal. In the bottom right corner, there are two overlapping circular patterns with thin white lines, resembling a stylized globe or a data visualization.



# State of the Cloud: 2021 Edition

- 1. Cloud is the default.**
- 2. Credential theft and misconfiguration remains the primary vector for attackers.**
- 3. Growing clouds mean more opportunities for mistakes.**
- 4. SaaS apps are mission-critical but not well understood.**



# As everything shifts toward the cloud, attackers are changing tactics:



Credential theft via phishing and leaks



Exploiting misconfigurations



Exploiting vulnerabilities in cloud-hosted apps

# Credentials Compromised in 11 Minutes



The image shows a screenshot of a tweet from Andrzej Dyjak (@andrzejdyjak) dated Nov 5. The tweet is a timeline for @github and contains a numbered list of events: 1. Pushing a commit with an AWS key at 15:27; 2. Receiving an email from @GitGuardian at 15:34 (7 minutes later) about a possible secret leakage; 3. The token being compromised for the first time at 15:38 (11 minutes after the push). Below the list, it says '3/8'. The tweet has 2 replies, 19 retweets, and 45 likes. A second tweet by the same user follows, stating that within the next 2 hours, there were 5 more alerts, with traffic coming from Germany, Netherlands, United Kingdom, and Ukraine, and that bots used Python and Node.js SDKs. A note at the bottom of the second tweet says: 'NOTE: I also received a security alert about vulnerable dependencies.'

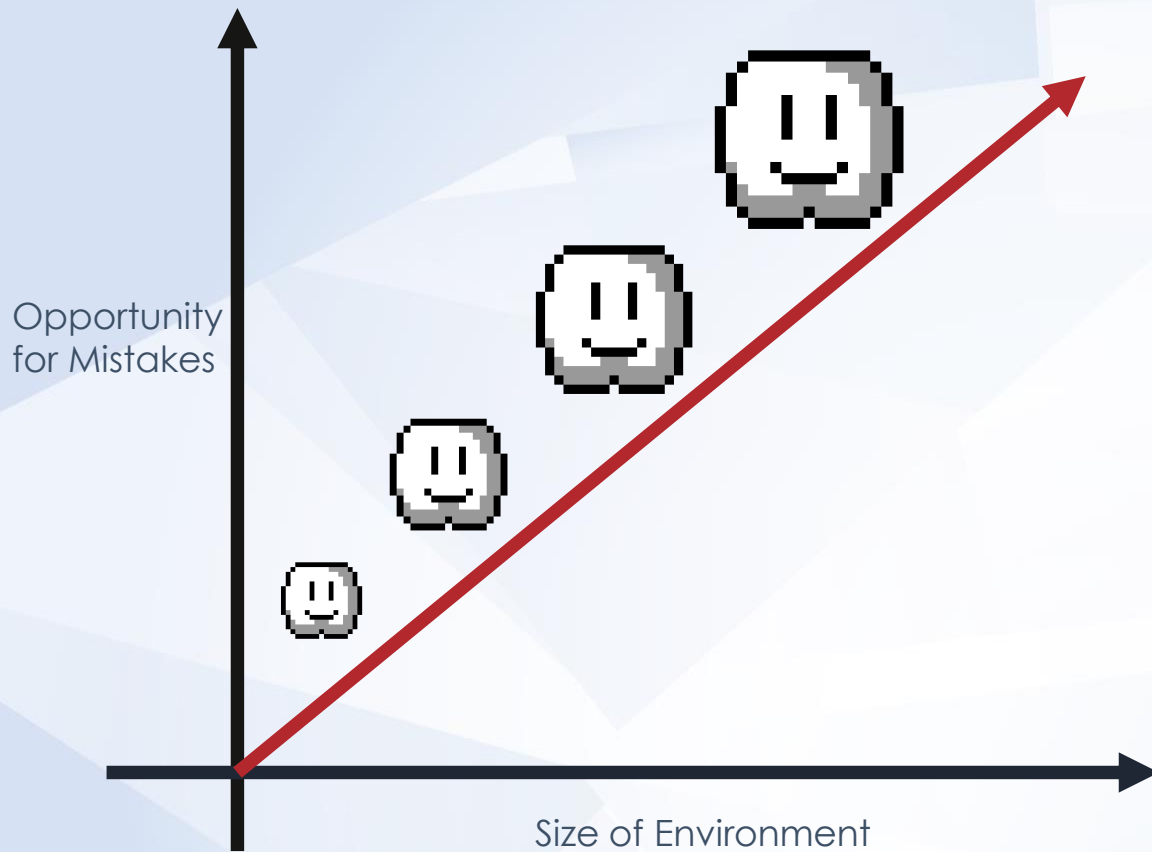
**Andrzej Dyjak** @andrzejdyjak · Nov 5  
Timeline for @github:  
1. I pushed the commit with AWS key at 15:27  
2. At 15:34 (7 minutes) I got an email from @GitGuardian informing me about possible secret leakage  
3. At 15:38 (11 minutes) the token was compromised for the first time.

3/8

2 19 45

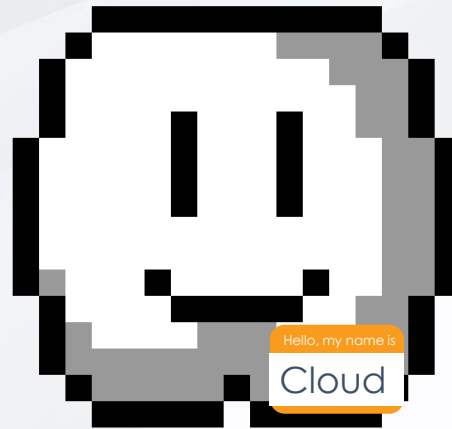
**Andrzej Dyjak** @andrzejdyjak · Nov 5  
Within next 2 hours there were 5 more alerts. Traffic came from: Germany, Netherlands, United Kingdom, and Ukraine. According to User-Agents bots used Python and Node.js SDKs.

NOTE: I also received a security alert about vulnerable dependencies.



As environments grow, the chances for misconfiguration grow with it.

**Cloud used to be simple.**

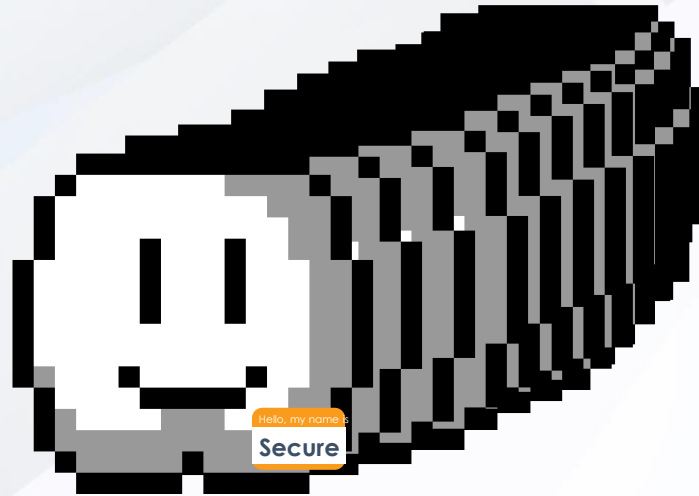


# 2021 has a multi-cloud problem.

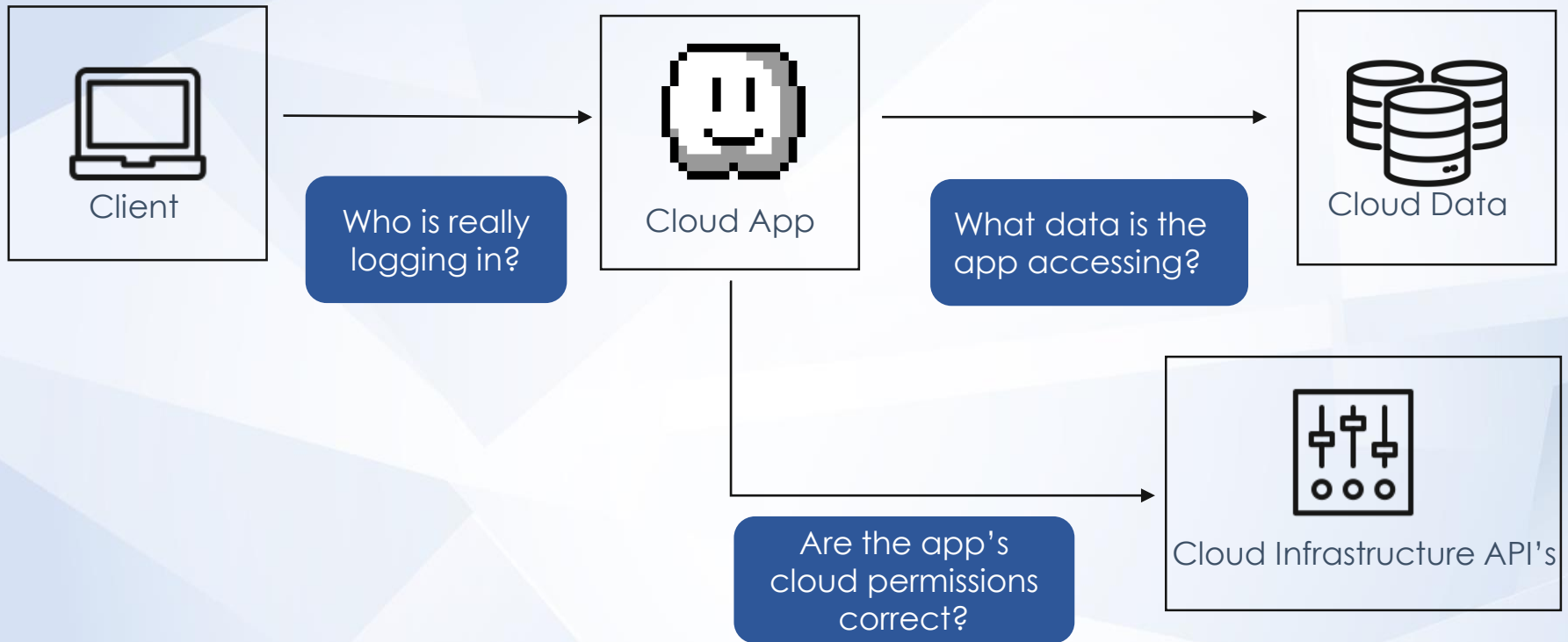


# It will need multi-cloud security solutions to make it manageable.

Orgs will need to reduce their interfaces of cloud visibility and control.



# Cloud apps need complete visibility and configuration management.





# Protecting Your Cloud Journey in 2021



**Step 4:** Validate your security controls and processes.



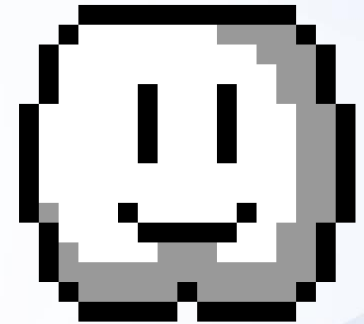
**Step 3:** Understand the actions of your cloud apps and services.



**Step 2:** Get visibility and control of the cloud infrastructure.



**Step 1:** Lock down your credentials.



**Q&A**

The background is a solid red color with several overlapping geometric shapes. On the right side, there is a large, light grey, angular shape that resembles a stylized letter 'M' or a similar symbol. Below this, there is a circle with a pattern of thin, parallel, dark grey diagonal lines. The overall composition is modern and abstract.



**Thank you!**

For more information, please visit  
[www.fireeye.com/predictions](http://www.fireeye.com/predictions)

## NEW CYBERSECURITY TRAINING STANDARD

- **HB852 (2.2-2009, I) for IT Security Awareness Training applies to executive, legislative and judicial branches.**
- **Agencies are now required to provide annual training using the curriculum developed by VITA. Agencies may develop additional training if needed.**
- **VITA shall assist agencies with implementing this requirement.**
- **Each agency must monitor and certify annual training activity and submit their certification to VITA on an annual basis.**
- **To address the requirements in HB852, VITA and the ISO council committee on IT security awareness training developed a new IT security standard, SEC527.**

# CORE REQUIREMENTS

**Agencies shall assure that they are providing cybersecurity awareness training that meets or exceeds the requirements identified in the Cybersecurity Awareness Training Standard 527 (SEC527).**

**Any cybersecurity training must cover the knowledge areas at a minimum. The names of the courses may change or be combined in other courses depending on the software solution or other solution that is chosen, but the knowledge areas identified in the SEC527 must be adequately covered.**

**SEC527 is currently on ORCA for public comment and review.**

## CYBERSECURITY CURRICULUM

**Agencies are required to procure, obtain or develop a cybersecurity curriculum that meets all of the requirements identified here:**

- ( A ) Core Requirements;**
- ( B ) Policy Review and Acceptance;**
- ( C ) Role Based Training;**
- ( D ) Other Regulatory Requirements;**
- ( E ) Phishing Exercise and optionally;**
- ( F ) Additional training where required**

## CORE REQUIREMENT COURSES

Separation of Duties

Security Incidents

Proper disposal of Data Storage Media

Proper Use of Encryption.

Access Controls, Secure Passwords

Working Remotely

Intellectual Property Rights

Security of Data

Phishing and Email

Social Engineering

Mobile Devices

Ethics

Least Privilege Identifying and Reporting

Privileged Access

Insider Threat

Cloud Services

Browsing Safely

Physical Security

Hacking

Personal Identifiable Information (PII)

Privacy

Social Network

Malware

## POLICY REVIEW AND ACCEPTANCE COURSES

*Require documentation of IT System users' acceptance of the agency's security policies. Cybersecurity awareness training must include policy review and acceptance*

---

**Acceptable Use - All users of IT systems must agree to the agency's acceptable use policy.**

**Remote Access Policy - All users of IT systems must agree to the agency's remote access usage and/or Telework Policy.**

**Other Applicable Policies - Users of IT systems must review and agree to comply with any applicable agency security policies.**



## ROLE BASED TRAINING

*Agencies must provide appropriate cybersecurity training based on the assigned roles and responsibilities of individuals with specific security requirements.*

---

**Data Owner Training**

**System Admin Training**

**Data Custodian Training**

**Agency Head Training**

## OTHER REGULATORY REQUIREMENT COURSES

*Agencies must provide training for all regulatory or contractual requirements that affect IT users. Agencies need to decide the appropriate level of regulatory training that is required for its users*

---

**Federal Tax Information (FTI)**

**Health Insurance Portability and Accountability Act (HIPAA)**

**Criminal Justice Informatin Services (CJIS)**

**Family Educational Rights and Privacy Act (FERPA)**

**Social Security Administration Training (SSA)**

**Payment Card Information (PCI)**

**Federal PII**

**Personal Health Information (PHI)**

## ADDITIONAL TRAINING WHERE REQUIRED

*Agencies should offer training that goes beyond the required curriculum items when necessary in the agency's environment. The items below are a few suggested additional training that agencies should consider for their employees where appropriate.*

*Senior Leadership Training*

*New Employee Orientation Training*

*Creating a Cyber Secure Home*

## PHISHING EXERCISE

**Agencies are required to conduct a phishing exercise or phishing training with their employee / contractor users. A phishing campaign will help identify if users can successfully recognize, avoid and report phishing attempts that may occur.**

**VITA will provide assistance in developing a phishing campaign for your agency if needed.**

*So far, none of this is really new.*

- *IT Security Awareness Training has been required in SEC501 for several years.*
- *Role-based training has been required in SEC501 for several years.*
- *Regulatory compliance training has been required in SEC501 for several years.*
- *Agreement to agency policies (i.e. acceptable use, remote access, etc) has been required in SEC501 for several years.*

*The new part is:*

- *There is now a new minimum level of training that needs to occur (the core requirements). The core requirements were agreed to by a committee of ISOs representing all 3 branches of state government (executive, legislative and judicial).*

*But the biggest change is:*

- *Agencies are now required to report their compliance for training to VITA on an annual basis.*
- *Agencies are also required to evaluate the efficacy of their training program to VITA.*
- *Agencies can also submit suggestions for improving training to VITA.*

## SECURITY AWARENESS TRAINING SOLUTIONS FOR CORE REQUIREMENTS

Software solution	Contact	Contact email
KnowBe4	Miesh Blankenship	mieshb@knowbe4.com
Awareity	Rick Shaw	rick.shaw@awareity.com
InfoSec	Dean Diercks	dean.diercks@infosecinstitute.com
SANS	Keeton Ellis	kellis@sans.org
Security Mentor	Dan Lohmann	dlohmann@securitymentor.com
Other vendor?	LET US KNOW!	
For DHRM LMS questions	Contact	Contact email
DHRM LMS	A. T. Hamilton	alexander.hamilton@dhrm.virginia.gov



## TIMELINE OF EVENTS

**January 1, 2021** – HB 852 went into effect. Agencies are required to provide annual information security training for each of its employees using the curriculum developed by the CIO.

**January 31, 2021** – Each agency is required to submit a form to VITA outlining the type of training solution the agency intends to use for CY 2021. If no training solution is being used, VITA will assist the agency in identifying a solution. However, due to the late date of publishing SEC527, we will extend the date to identify your training solution to **February 28, 2021**. In lieu of a form, this information can be submitted directly in Archer (soon). All we're looking for here is your agency's plan of what you intend to do for training in CY2021.

**January 31 through March 31, 2021** – VITA will review and approve agency training solutions. VITA will develop remediation plans for agency training programs that are judged not to meet minimum requirements

**January 1, 2021 through December 31, 2021** – Agencies should be training their employees and contractors (same as always).

**January 31, 2022** - Agencies must submit to VITA a statement of compliance with the cybersecurity training standard and their suggestions for improvement. There is a form for this and it will also be available in Archer.

# QUESTIONS?

[Tina.gaines@vita.Virginia.gov](mailto:Tina.gaines@vita.Virginia.gov)

[Edward.miller@vita.Virginia.gov](mailto:Edward.miller@vita.Virginia.gov)





# UPCOMING EVENTS

## FEBRUARY 2021 ISOAG MEETING

Feb. 3 from 1 – 4 p.m.

Webex

Rick Shaw, Awareity

Michael D'Arezzo, ePlus Technologies

Dennis Moreau, Vmare



# ADJOURN

THANK YOU FOR ATTENDING!

