ESG Brief

Cybersecurity Predictions for 2020

Date: December 2019 **Author:** Jon Oltsik, Senior Principal Analyst and ESG Fellow; Doug Cahill, Senior Analyst and Group Director; Christina Richmond, Principal Analyst; Dave Gruber, Senior Analyst; and John Grady, Analyst

Abstract: The ESG cybersecurity analyst team got together recently to discuss our top predictions for 2020. This brief details our predictions in three categories: threats, technology, and the cybersecurity community (i.e., cybersecurity professionals and the industry at large).

Overview

ESG looks forward to 2020 with grave concerns. Threat actors continue to grow more sophisticated, while the attack surface increases, driven by cloud computing, digital transformation, networked business processes, and IoT devices. At the same time, organizations face a consistent set of cybersecurity problems—they have too many tools, too many manual processes, and a shortage of bodies and advanced skills.

ESG sees 2020 as a year of transition, as CISOs seek scalable, intelligent, and automated solutions that can greatly improve security efficacy, operational efficiency, and business enablement. Buckle up—2020 is likely to be a bumpy ride!

2020 Predictions

The ESG cybersecurity analyst team gathered together to compare and collaborate on our cybersecurity predictions for 2020. After a lot of discussion and debate, we came up with the following list across three categories: threats, technology, and the cybersecurity community.

The Threat Landscape for 2020

As stated previously, threats will become even more sophisticated in 2020, taking advantage of an ever-growing attack surface. This will lead to a situation where:

- **Business email compromises (BEC) and other types of cyber fraud will continue to grow across industries.** A business email compromise is an exploit where a cyber-adversary gains access to corporate email accounts and then assumes a manager or executive's identity to fool employees into paying phony bills, transferring funds, etc. Some industry research indicates that BECs grew 2x to 3x in 2019, and ESG believes it will become even more pervasive in 2020 for one reason—BEC works. In the past, BECs were most prevalent in the financial services industry and real estate, where large transactions are conducted online. Cybercriminals will emulate these attacks across other industries in 2020, with a focus on industries like academia and state/local government agencies with limited cybersecurity

training and high turnover. ESG's Dave Gruber expects smaller payouts but heavier BEC volume next year. Other types of fraudulent cyber activity, including those that exploit the broad use of cloud applications to route payments to personal accounts, will also increase in 2020.

- **At least three US States will declare states of emergency due to waves of ransomware.** In July 2019, Louisiana Governor John Bel Edwards declared a state of emergency as a response to destructive ransomware attacks on three public school districts. While the state of Texas didn't follow suit, agencies in 22 towns in that state suffered a similar fate in August. All in all, ransomware will carry a price tag of over $10 billion this year. Ransomware will continue to plague state and municipal agencies lacking appropriate skills, controls, and ransomware countermeasures. This situation will come to a head in 2020 as at least three additional US states suffer infestations of ransomware attacks and declare states of emergency in response. Will this escalate to a national level? ESG gives this possibility a 20% chance. Washington DC remains way behind on cybersecurity knowledge and action so it's unlikely, but if the right swing states are attacked in an election year, legislators from both parties may be more willing to offer federal assistance.

- **Mobile malware will continue its rise.** Smartphones have become an essential tool for mobile banking, payments, and health care management. Additionally, mobile and IoT devices are becoming more pervasive in all types of networks: home, corporate, government, and critical infrastructure. This has led to a rise in mobile malware over the past few years, including the Anubis banking Trojan, and the TimpDoor phishing attack. Given the growing attack surface and limited mobile security protection, ESG expects a rapid rise in mobile malware to follow in 2020. While consumers will remain the primary focus, ESG also expects ambitious cyber-adversaries to include mobile attack vectors for possible targeted attacks in 2020 through social engineering and business-focused mobile phishing attacks. CISOs should assess mobile security and user knowledge as they prepare their 2020 cybersecurity budgets and strategies.

- **Targeted disinformation and deep fake videos will become mainstream**. Disinformation, false information spread deliberately to deceive a person or group, has become synonymous with democratic elections worldwide. According to recent ESG research, 42% of registered voters in the US say they are certain that they have come across political disinformation, 28% are pretty sure that they have, and 18% say it is probable that they have but they aren't certain.[1] Disinformation extends beyond politics, however, as the recent attack on the Olive Garden restaurant chain illustrates. ESG believes that in 2020, disinformation and deep fake videos (an AI-based technology used to produce or alter video content and present false content that did not occur), will be used more extensively for attacking the private sector. It's likely that these techniques will appear as part of blended threats in ransomware campaigns as well. As 2020 approaches, organizations should consider these expanding threat vectors as part of their incident response planning.

- **Serverless APIs will come under attack.** When it comes to security and compliance, cloud service providers (CSPs) have always emphasized the shared responsibility model. CSPs are responsible for security "of the cloud" and customers are responsible for security "in the cloud." This demarcation always made sense in the past, but it is currently evolving, as serverless computing services like AWS Lambda emerge as popular event-driven programming models. Changes to the shared responsibility model make assets more dynamic and ephemeral, turning application code into infrastructure, oft referred to as infrastructure-as-code. There are many moving parts to this model and a large percentage of organizations continue to lack the appropriate cloud security knowledge and skills to keep up. This presents a "perfect storm" threat vector for cyber-adversaries in 2020. Like cloud workload misconfiguration attacks à la Capital One, ESG believes at least one large targeted attack and/or data breach in 2020 will be the result of serverless/API-level attacks. This growing threat vector will be a major topic for users and vendors in 2020, as well.

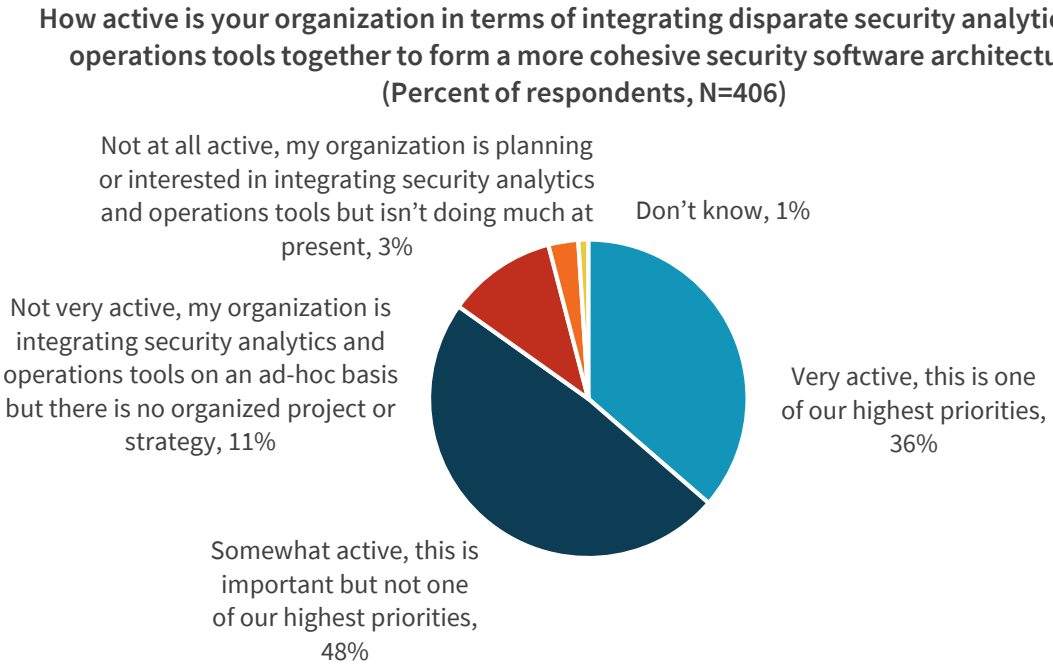
[1] Source: ESG Brief, *Voters Agree: Political Disinformation is Real, Omnipresent, and Troubling*, November 2019.

Cybersecurity Technology Developments in 2020

ESG believes that every layer of the cybersecurity technology stack is in a state of transition, leading to golden opportunities for technology vendors. Alternatively, many users will remain confused about what technologies to replace and/or supplement, and when to do this. ESG will monitor cybersecurity technology trends in 2020, including:

- **Converging cybersecurity technology stacks.** Architectures and integrated platforms will continue to supersede best-of-breed point tools in 2020. For example, security operations and analytics platform architecture (SOAPA) will gain momentum in security operation centers (SOCs). This is already happening. According to ESG research, 36% of organizations say they have a very active SOAPA integration effort, and it is one of their highest priorities (see Figure 1).[2] SOAPA integration will gain momentum in 2020 as security technology stacks migrate to the public cloud or become part of XDR (threat detection and response suites). This same type of convergence will also impact network security as individual controls like firewalls, VPNs, DNS security services, DLP, and web security evolve from products to services as part of cloud-based elastic cloud gateways (ECGs). ECGs will also include networking services like SD-WAN and WAN optimization. ESG expects robust ECG growth in 2020 to align with the changing security needs of hybrid IT, mobile workers, and IoT device growth. Similarly, while cloud security is a relative newcomer to other cybersecurity product categories, ESG expects convergence in this market segment as well. To that point, container security is and will continue to become a feature of cloud workload protection platforms (CWPPs) and ESG predicts that CWPPs will merge with cloud security posture management (CSPM) solutions representing the arrival of cloud security platforms.

Figure 1. Security Analytics and Operations Tools Integration



Source: Enterprise Strategy Group

- **Vulnerability management will become a nexus for AI and automation.** When asked to identify their organization's primary security operations objectives, 40% of security professionals said they want to improve their ability to

[2] Source: ESG Research Report, *The Rise of Cloud-based Security Analytics and Operations Technologies*, to be published. All other ESG research and references have been taken from this research report, unless otherwise noted.

discover, prioritize, and remediate software vulnerabilities. In fact, vulnerability management has been problematic for years. Scanning tools regularly uncover thousands of software vulnerabilities across the enterprise, leaving IT operations teams dumbfounded about which ones to prioritize and remediate. To address this omnipresent situation, organizations will supplement vulnerability scanners with AI/ML and process automation (SOAR) in 2020. Tools from vendors like Kenna Security and Tenable Networks will help organizations prioritize critical software patching based upon algorithms that consider threat intelligence and exploitability factors to calculate risk scores. Armed with this knowledge, IT operations staff will work through patching activities using runbooks and process automation tools from Demisto, IBM, Lastline, ServiceNow, Splunk (Phantom), and others. While these technologies aren't new, vulnerability management will become a hotbed of activity in 2020 as AI, automation, and vulnerability scanners are tightly integrated and offered as bundled suites or managed services.

- **Enterprise-wide IAM mega-projects.** Identity and access management (IAM) infrastructure has long been glued together in a piecemeal and inefficient fashion. This is often because many groups own pieces of IAM infrastructure (such as application developers, IT operations, and cybersecurity), but no one is responsible for the whole thing. The broad use of cloud applications and services exacerbates these identity and access management governance challenges, with identities often stored in cloud silos. A notable side effect of cloud identities is the proliferation of privileged accounts, including service accounts. While this won't change, ESG does expect many large organizations to scope out plans to replace the legacy patchwork of IAM tools with cloud-based enterprise IAM solutions in 2020 for several reasons. First, existing IAM infrastructure is too cumbersome to accommodate mobile applications, heterogeneous clouds, and growing populations of employee and non-employee users, creating a business requirement for change. Second, employees and non-employees walk around with mobile phones built with biometric technologies and authentication standards like FIDO, instrumenting the IAM architecture for strong authentication. Finally, cloud-based highly scalable identity engines from Amazon, Google, Microsoft, Octa, Ping, and VMware will ease the transition. ESG expects that these IAM projects will also include a fresh take on privileged access management (PAM) for implementing least privilege policies to limit which users get access to high-value cloud-based applications and services. These projects will begin in 2020 but will take two to three years to complete. Nevertheless, 2020 will be notable as the year for identity modernization as IAM moves to the cloud.

- **A big year for threat intelligence and hunting, and the increasing prominence of the MITRE ATT&CK framework.** Eighty-two percent of security professionals say that improving threat detection is a high priority in their organization.[3] This often equates to detecting attacks in real time, but comprehensive threat detection should also include retrospective investigations, digital forensics, and proactive threat hunting. CISOs are starting to recognize that they need to do more around threat intelligence, beyond simply blocking high-risk IoCs. In 2020, many enterprises will establish formal threat intelligence programs, using things like the MITRE ATT&CK framework and threat intelligence analytics and activity hubs (TIAAs) from vendors like Anomali, RecordedFuture, ThreatConnect, and ThreatQuotient. Once again, the global cybersecurity skills shortage will likely put a damper on hiring plans, so most organizations will opt instead for managed security services. In fact, 44% of organizations use or plan to use managed services for threat intelligence analytics while 30% use or plan to use managed services for proactive threat hunting. This will only rise in 2020: Ninety-one percent of organizations indicate that they will increase their use of managed security services in the future.

Cybersecurity Community Developments in 2020

The cybersecurity community includes security professionals, service providers, and technology vendors. Within this community, ESG's expectations for 2020 include:

[3] Source: ESG Master Survey Results, *The Threat Detection and Response Landscape*, April 2019.

- **Massive salary inflation for cloud security experts**. Organizations are aggressively moving workloads to the public cloud, creating a hybrid IT architecture. This has created strong demand for new security positions like cloud security architects and engineers, but individuals with these skills are in short supply. According to research from ESG and the Information Systems Security Association (ISSA), one-third of cybersecurity professionals claim that of all security skills deficits, cloud security skills represent one of the biggest shortfalls.[4] While many security professionals are pursuing cloud security certifications at present, ESG expects the cloud security skills gap to increase in 2020. Organizations desperate for cloud security skills will compete for talent by boosting salaries and benefits, leading to massive salary inflation. This in turn will cause several ripple effects. To take advantage of lucrative opportunities, seasoned security professionals will seek out cloud training and certification programs while experienced cloud security professionals will be recruited away from steady jobs, leading to high attrition rates and unforeseen internal skills deficits. Look for cloud security training to be highlighted at Black Hat in August when chaos caused by the cloud security skills discrepancy is widespread.

- **A focus on cyber-risk and decreasing the attack surface.** While much of cybersecurity centered on threat detection and response in the past, ESG believes that organizations will increase their focus on cyber-risk in 2020. This will drive a need for granular visibility into all network nodes, real-time knowledge of the threat landscape, and a true understanding of which assets are truly vulnerable. At present, no single analytics tool can provide this level of cyber-risk detail (note: this is a huge opportunity), so CISOs will increase spending next year in areas like continuous automated penetration and attack testing (CAPAT) tools (like AttackIQ, Cymulate, Randori, SafeBreach, Verodin [FireEye], and XM Cyber) that assess security controls and attack preparation. As previously mentioned, ESG also expects a lot of action around vulnerability management integration related to scanners, process automation/SOAR tools, and AI/ML. As part of their focus on cyber-risk management, CISOs will also make decreasing the attack surface a high priority in 2020. This effort will encourage projects in areas like DNS security services (such as Cisco Umbrella, and Infoblox), and zero-trust networking initiatives (such as software-defined perimeter [SDP] and micro-segmentation projects with vendors like Cyxtera, Illumio, Palo Alto Networks, Privafy, vArmour, and Zscaler). Expect organizations to get back to basics as well, with renewed efforts around security hygiene like the CIS Top 20, and OWASP Top 10.

- **Cloud service providers (CSPs) will become cybersecurity hubs.** While the shared cloud security model persists, major cloud service providers continue to increase their security technology and services offering. For example, Google (Chronicle Backstory) and Microsoft (Azure Sentinel) introduced cloud-based security analytics in 2019 with Amazon rumored to do the same before year's end. Each CSP has also increased basic security capabilities within their cloud environments. At AWS Re:Inforce in June, Amazon rolled out a series of announcements in areas like VPC traffic monitoring, multi-factor authentication (MFA), and Kubernetes security. Similarly, Google announced several security upgrades including Google Premium edition, a bundle of its cloud security command center and event threat detection capabilities. At Ignite, Microsoft stressed Azure Security Center for posture management, MFA, and new defenses against insider threats, while hybrid IT trailblazer VMware recently rounded out its security portfolio through the acquisition of Carbon Black. Moving forward in 2020, organizations will further define their IT architecture for the coming decade and select primary cloud vendor partners. As this happens, budget dollars will migrate from standalone cloud security technology vendors to CSPs. Cybersecurity vendors who allow organizations to unify their security policies across the disparate infrastructures of hybrid, multi-clouds (for example, firewall management, and data loss prevention) will be increasingly viewed as strategic by providing important functionality not available from the hyperscale CSPs.

[4] Source: ESG Research Report, *The Life and Times of Cybersecurity Professionals 2018*, May 2019.

- **M&A activity.** 2019 has been a hotbed of M&A within the cybersecurity industry. Palo Alto Networks grabbed Demisto, Twistlock, PureSec, and Zingbox. Trend Micro purchased Cloud Conformity. Carbonite acquired Webroot in March, and then the newly formed conglomerate was purchased by OpenText. Symantec was gobbled up by Broadcom while PE firm Thoma Bravo bought Sophos. ESG expects increased M&A activity in 2020 as large platform vendors fill gaps in their portfolios in areas like:
    - **Endpoint security.** There are still a few independents like Cybereason and SentinelOne that could extend a larger vendor's portfolio.
    - **Network traffic analysis.** There are many strong products from vendors including Corelight, DarkTrace, and Vectra Networks. These software tools may become sensors for broader security analytics firms and services.
    - **Cloud security.** Container security companies such as Aporeto, Aqua Security, NeuVector, and StackRox; CWPP vendors such as Capsule8, Lacework, and Threat Stack; and CSPM vendors including DivvyCloud, Fugue, and CloudCheckr are all on the list of corporate development executives and investment bankers alike.
    - **AI/ML analytics.** As AI/ML analytics becomes a product feature rather than a standalone market, many specialty shops will be scooped up.
    - **CAPAT**. As this market heats up, ESG expects CAPAT to become a core component of cyber-risk management platforms.
    - **Deception technologies.** This is a nascent market but it is growing in usage and value. A few small acquisitions are possible here.
    - **TIAA.** Threat intelligence analytics and activity hubs are appreciated by enterprise customers yet remain somewhat undervalued in the market. The exception here is RecordedFuture, which was acquired by Insight Partners in May 2019. ESG expects more of the same in 2020.

The Bigger Truth

ESG expects an eventful 2020 in cybersecurity. Attacks will grow more sophisticated and further integrate social networking and deep fake components. Meanwhile, the attack surface continues to grow unabated. On the technology side, ESG expects strong momentum around tools integration and automation, and growing incorporation of artificial intelligence and machine learning into threat prevention and detection tools. Finally, ESG sees an increasing enterprise focus on cyber-risk management, leading to changes in processes, priorities, and investments.

CISOs should prepare for new types of threats, security technology architectural changes, and an increasing dependence on third-party service providers. 2020 promises to be exciting, innovative, transitional, and alarming. Happy new year!