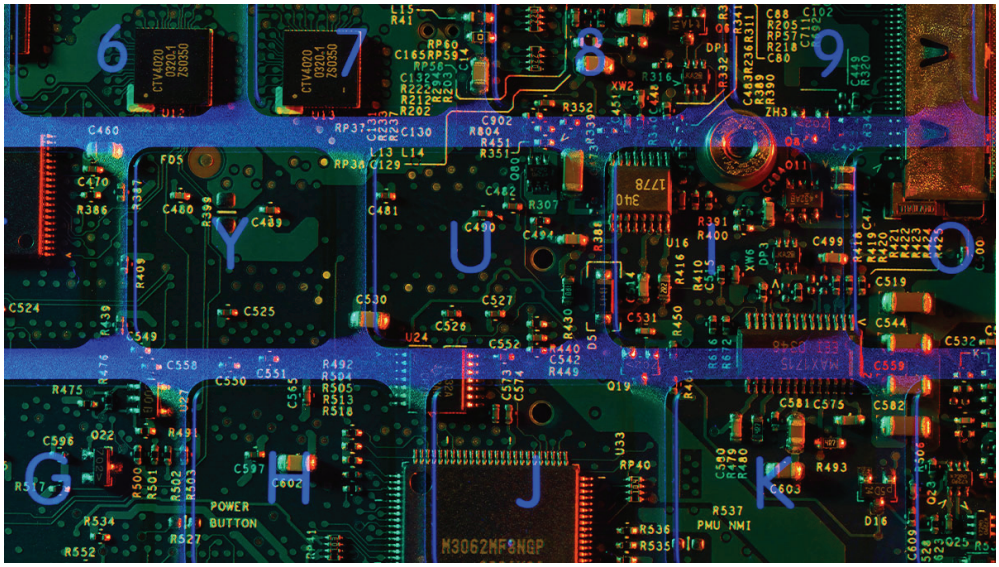
Where to Focus Your Company's Limited Cybersecurity Budget

Three cybersecurity investments to target. **by Adam Isles**

Published on HBR.org / May 23, 2023 / Reprint H07NF0



Rafe Swan/Getty Images

Recent research indicates that organizations with 10,000 or more employees typically maintain almost 100 security tools. And yet, well-established global companies continue to be victimized by cyber attacks. For example, payments-processor NCR recently experienced a ransomware attack that caused downstream outages across numerous restaurant back-office and point-of-sale systems. With the prospect of a 2023 recession, reporting suggests that chief information security officers (CISOs) will increasingly see budgets constrained. So how

can companies focus their limited cybersecurity investments on the controls that matter most?

Given that cyber risk operates within the context of a highly dynamic threat, business, and technology environment, it's important to set some context for how we will measure cybersecurity performance. As Michael Chertoff recently noted, good cybersecurity programs operate with a high degree of transparency, accuracy, and precision.

The Elements of a Good Cybersecurity Program

Transparency comes from using authoritative security frameworks from places like the U.S. National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO) that are repeatable and auditable. That said, these frameworks typically define practices at a high level of abstraction ("remote access is managed" … how?) and need to be married with a more detailed analysis of likely threat techniques to ensure that security defensives *accurately* map to these threats. We also need to be *precise* about the attack surface we address with a particular control.

Different defenses will apply depending on the type of attack surface: laptop operating systems, web servers, remote-user-assist technologies, cloud technologies, or user-productivity-software like browsers and email, all of which can be compromised by bad actors to achieve initial access to your company's systems.

With this in mind, we can break cybersecurity investments into three categories: 1) controls that defend against threats in a particularly impactful way, 2) measures that validate that these controls are operating as intended and 3) capabilities that automate the other two.

Controls That Defend Against Threats in Impactful Ways

Where should companies start? In the same way that doctors use patient profiles to prioritize preventive measures, and diagnostics and therapies to manage patient-specific risks, we can use business profiles to help us understand the spectrum of potential threats. As with Covid-19, ransomware is a risk that applies universally, but some organizations (e.g., technology providers) also need to be concerned that they could be targeted as steppingstones into customer environments, as in the recent widely-reported 3CX hack. With this in mind, we can focus on controls that defend against those threats.

It's easy for threat actors to change the signatures of an attack (things like malware code that antivirus systems can detect). It is much more difficult for attackers to change their underlying methodologies, known as tactics, techniques, and procedures (TTPs). The MITRE Corporation's Adversarial Tactics Techniques & Common Knowledge (ATT&CK) framework is the most comprehensive, authoritative approach to cataloguing threat actors, their motivations and TTPs that is openly available today – and it's free to use. Companies can use ATT&CK to familiarize themselves with the threat techniques they need to defend against based on their business profile. ATT&CK also maps each technique to a corresponding security countermeasure, helping to align investments with threats.

Minimizing Initial Access.
A baseline step is to minimize the likelihood that an adversary can achieve initial access. ATT&CK tells us that there are nine ways threat actors can get inside a target organization — including phishing, the abuse of external remote services, and compromises of valid accounts. Companies need to consider all nine of these potential access points and either address them or consciously accept the risk of not doing so, and prioritize how appropriate controls are phased in.

Mandiant's latest annual M-Trends report indicates that exploitation of vulnerabilities on public-facing applications (such as software flaws that enable threat actors to bypass authentication and remotely execute code) is the most common initial access technique observed across its investigations, so resources that patch internet-reachable vulnerabilities are a particularly impactful control. For cloud-centric environments, recent research from Google indicates that valid account compromise (either through weak credentials or leaked credentials) make up well over half of all incidents observed on its platform, highlighting the urgency of multifactor authentication (MFA) solutions (especially as organizations migrate workloads to cloud environments).

Defense in depth.
Companies need to plan for contingencies where an attacker achieves initial access, perhaps by finding an internet-facing machine without MFA or by tricking someone into visiting an infected website. *What then?*

We can use ATT&CK's knowledge base to flag and address techniques that are commonly used across threat actor groups with a foothold inside the target organization. These techniques can represent "chokepoints" that, if disrupted, can illuminate or defeat the adversary's campaign. For example, threat reporting from Mandiant, Red Canary and Picus Labs all highlight how bad actors have used command and scripting interpreters like PowerShell to execute commands or scripts. The threat actors responsible for the Solar Winds breach used PowerShell and Windows command line throughout the entire campaign. By baselining "normal" command and scripting activity and users, companies can detect and respond to malicious use of this technology.

ATT&CK's library also flags controls that give broad coverage against behaviors that threat actors are likely to use. For example, many

of the data sources needed to detect a broad swath of threatening behaviors are captured and analyzed by endpoint detection and response (EDR) tools, which provide visibility and automated responses to sophisticated intrusions by matching system events against known adversarial behaviors (including above-referenced command and scripting interpreter techniques).

Precision also involves focusing the deployment of such tools where they matter most: on an organization's "high value assets." Definitions can be hard, but certain systems are highly targeted by threat actors because they perform functions critical to trust and are thus stepping-stones into everything else. After the SolarWinds incident, the U.S. National Institute of Standards and Technology (NIST) defined such a list of critical software.

For example, identity and access systems fall within NIST's definition: they are key defenses in their own right, and incident data demonstrates that threat actors often work to capture highly privileged credentials on centralized access control systems like Microsoft Active Directory, with devastating results. Once credentials are in hand, the adversary is posing as a legitimate credential holder, and follow-on activity is much more difficult to detect. Maintaining the integrity of these systems is thus a key priority.

Resiliency.
For high-value assets, investment in controls like off-line back-ups that enable survivability are of paramount importance, especially in low-probability, high-consequence scenarios where no decryption is possible. For example, in November 2022, Microsoft reported that a variant of destructive malware campaigns widely seen in Ukraine since the start of the war was now being used to attack logistics organizations in Poland.

Controls Validation

In our work with clients, we have found that controls are often not fully deployed or operating as expected. Our experience is not unique, and this is why the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) have jointly recommended validating control effectiveness. The same threat-modeling process described above can also be used to focus testing efforts on emulating relevant threat techniques to ensure that your company's controls are working as intended.

Automation

Attempting to manually manage, validate, remediate, and track security posture — i.e., determining where, exactly, security controls are deployed and whether they are operating as intended — is becoming difficult to impossible. A recent survey highlighted that organizations continue to experience rapid growth in technology environments (2022-to-2023 increases were typically 137% for applications, 188% for devices, and almost 30% for users) and risk (a 589% 2022-to-2023 increase in security findings). The total global volume of data is estimated to reach 175 zettabytes (one zettabyte is equivalent to a trillion gigabytes) by 2025 (versus 33 zettabytes in 2018).

Strengthening security will thus increasingly involve automation. Security Orchestration and Automated Response (SOAR) tooling is already well-known within the security community, as are automated software updates where practicable (which are more easily handled for endpoint operating systems and productivity technologies like browsers). Three other forms of automation are worth highlighting:

1. Tracking an asset's posture and any related decay (for example, where internet-facing servers are left exposed online without a password,

which has repeatedly happened in cloud environments), particularly for internet-facing technologies.
2. Evaluating coverage against changing threats.
3. Threat-emulation testing, where threats are simulated through automated scripts on relevant systems. Not only will automation help better secure organizations, it should also help reduce the number of security findings in need of remediation (catnip to plaintiff's lawyers and regulatory agencies in the event of an incident).

Companies can start by identifying where automation functionality exists within larger IT solutions. Tracking asset posture can often be achieved through native IT asset and service management technologies, as well as through out-of-the-box tools from cloud providers, for example Microsoft's Secure Score. Some cloud systems such as Google Cloud Platform have started to map posture to controls frameworks published by NIST and the Center for Internet Security.

As business profile, attack surface complexity, and related threats change, so too will the relative value of specific controls. A foundational step in addressing which controls matter most is thus tracking how underlying business, technology, and threat factors are changing, and what that means for security.

This article was originally published online on May 23, 2023.

Adam Isles is principal and head of the cybersecurity practice at the Chertoff Group, where he advises clients on managing security and safety risk. Previously, Adam served as the Deputy Chief of Staff at the U.S. Department of Homeland Security (DHS) from 2007-2009. Before joining DHS, Adam served at the U.S. Department of Justice, where he started his legal career as a trial attorney in the Criminal Division in 1997. Adam is a Certified Information Systems Security Professional (CISSP), and he graduated from Harvard Law School in 1997.

