SECRUTINY

5 Cybersecurity Must Haves

Secrutiny Report

March 2022

CHARITY IT LEADERS

Introduction

In many ways, 2021 was a challenging year for cybersecurity. Solar Winds, Colonial Pipeline, and many other high-profile breaches had significant economic and security consequences. Ransomware struck with a vengeance, targeting many small and medium-sized enterprises. Perhaps most concerning was how adversaries targeted and exploited critical infrastructure and supply chain security flaws at a faster rate than in the past.

It led many cybersecurity professionals to question what they should prioritise to be better protected from an attack in the first instance and what would offer the best assurance they will survive an incident should the worst happen.

Secrutiny has developed this guide to the top cybersecurity must-haves – the five things we should all be doing or looking to invest in over the years.

CHARITY IT LEADERS

We'd like to thank our platinum sponsor Secrutiny for producing this very accessible guide to the top 5 things you should be considering to secure your organisation for the long term.

We're all being asked to do more with less, so investment has to be targeted in the right areas, and these recommendations will help you target your cybersecurity roadmap.

Tree Hall and Matt Jago

1 | Multi-Factor Authentication

Add MFA to everything

With the rise in sophistication of credential-related threats such as social engineering and brute force, passwords just aren't secure enough anymore. And the consequences of a breached credential can be devastating for any business. Multi-factor authentication (MFA) is an extremely low-cost high-reward cybersecurity control.

Even if it's only a two-factor authentication and forcing a peremptory challenge so that more than just a password is required creates an obstacle that an attacker may not be able to get around. Often this can be implemented relatively easy as most domains are being managed by Active Directory (AD) and, in most cases today, by Azure AD.

So, it's a service enablement feature that then gets pushed down through AD authentications to services.

MFA is now commonly a minimum requirement for cyber insurance. Stated bluntly: if MFA is not enabled in your environment, you are engaging in behaviour so risky that cyber insurance carriers will not offer coverage to your business.

2 | Email Security

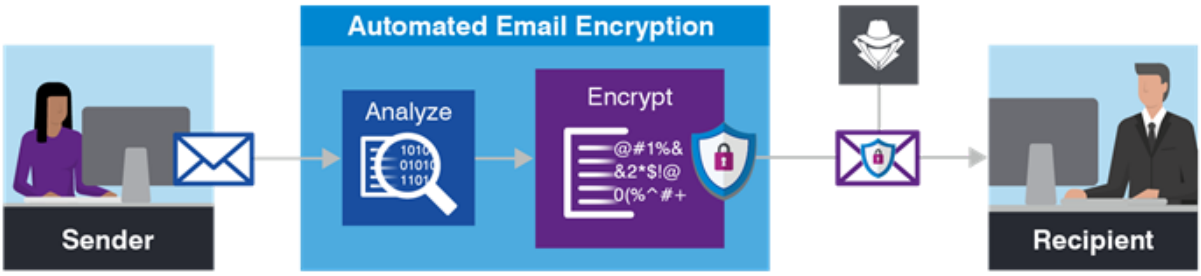
Phishing email remains the no. 1 attack vector

Email is your most essential business tool—and today's number one threat vector, and the threat it poses changes and evolves more rapidly than ever before. Attackers know the most straightforward way into your organisation is through your people and their email and cloud accounts, rather than systems and infrastructure. Yet, email security at more than 40% of businesses falls short in one or more critical areas, and 13% of businesses don't have an email security system at all[1].

One of the first email security best practices you should implement is a secure email gateway, either on-premises or in the cloud, to offer multi-layered protection from unwanted, malicious and BEC email; granular visibility; and business continuity.

It may also be important to deploy an automated email encryption solution as a best practice to reduce the risks associated with regulatory violations, data loss and corporate policy violations while enabling essential business communications. This solution should be able to analyse all outbound email traffic to determine whether the material is sensitive. If the content is sensitive, it needs to be encrypted before being emailed to the intended recipient. It's especially important for organisations required to follow compliance regulations, like GDPR, HIPAA or SOX, or abide by security standards like PCI-DSS.

[1] The State of Email Security 2021 Report



Your users are a fundamental line of defence inside the perimeter to help defeat attacks using social engineering to compromise accounts. Awareness Training can help dramatically reduce risk related to human error, but technology controls are essential to counter insider email threats.

3 | Just-in-time-administration

74% of breached organisations admit that their breach involved a compromised privilege credential

Prevalent standing privilege (those administrator accounts with “always-on” 24x7x365 privileged access) increase your attack surface because they’re the primary mode of ransomware spread, with each one offering an opening to move laterally.

Even with privileged access management (PAM), you can only protect known privilege. You have no visibility into the sprawl of administrator access that exists outside the vault, and more importantly, available to an attacker from the average employee workstation.

Wouldn’t it be better to grant authorised users the privileged access they need for the minimum time and only the minimum rights they need? Zero standing privilege is an emerging approach based on administering privileged access, across your entire IT and Security ecosystems, on a Just-In-Time, Just-Enough basis using MFA to authenticate the request.

4 | Immutable Backups

It should be no. 1 if you have the money...

One of the most pressing risks facing every organisation today is the threat of a ransomware attack. And unfortunately, it looks like it's here to stay:

- Ransomware is up 150% since the beginning of 2021, with an estimated impact of $1.4 billion. (Forbes).
- By the end of 2021, a new organisation will fall victim to ransomware "every 11 seconds". (Cybercrime Magazine).
- On average, companies experience 21 days of downtime after a ransomware attack. (Coveware).

As if this wasn't scary enough, in more and more cases, as well as attacking your critical systems and data, every backup is deleted or encrypted. So, how do you ensure that your backup data is not vulnerable?

While primary storage systems must be open and available to client systems, your backup data should be isolated and immutable. An immutable backup is simply stored digital data that, once saved, is fixed and unchangeable—and cannot be overwritten or deleted. It's the only way to ensure recovery when production systems are compromised.

Data protection goes well beyond simple file permissions, folder ACLs, or storage protocols. Because these protocols are not entirely secure and can be circumvented, immutability must be integral to your backup architecture and not be bolted on after the fact.

In addition to protecting against malicious data corruption, having an immutable backup helps you conform with regulatory data-compliance requirements—ensuring that accurate copies of data are retained.

5 | Centralised & Secure Logs

You don't want to be blind if there is a suspected incident

Industry analysis will show high percentage statistics about most breaches remaining undiscovered for a few hundred days. More specifically, 256 days based on IBMs 2020 findings UK and globally on the 'time to identify & contain'.

With these numbers, why would you only retain logs for 90 days? Don't you want end-to-end visibility to find emerging IOC that may have existed in your environment many months ago? Probably because traditional SIEMs typically come with pricing uncertainty as most services are billed on an events-per-second or data volume model.

Yet the nature of cybersecurity encourages increased log sources from as many controls as possible, including cloud-based services such as M365. Evidence shows the requirement is between 1-2 years of log data for a better-equipped incident response function to give extensive backwards cover.

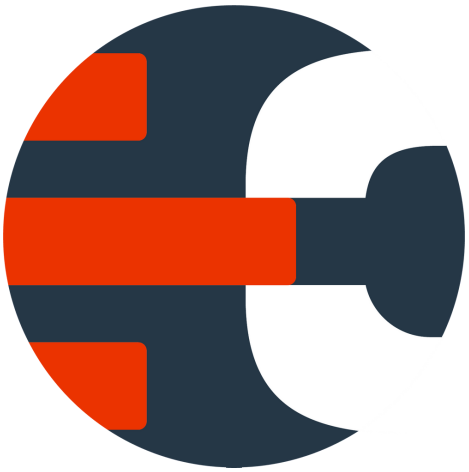
To overcome this pricing uncertainty challenge, Secrutiny has teamed up with Google Cloud Security to use its innovative Chronicle platform to make security analytics instant, easy, and cost-effective.

Modern security requirments:

- Lower and predictable TCO
- Petabyte scalability
- Security analytics at the speed of Google search
- On-premise and hybrid cloud visibility
- SOC productivity multipliers

Chronicle is a specialised, cloud-native security analytics system built on the core infrastructure that powers Google itself. Customers upload their security telemetry to a private instance within the cloud platform, where it is automatically correlated to known threats based on both proprietary and third-party signals allowing security professionals to analyse petabytes of telemetry at the speed of search.

Who are Secrutiny?



Secrutiny is an MSSP that believes cybersecurity doesn't have to be complex to be smart. The right balance between prevent, detect, respond, and recover offers the best assurance that your operation will survive an incident.

We encourage and guide you through identifying risk, determining effective policy and processes, and architecting security solutions that work in your environment and don't slow your operation down.

Our core services include – Cyber Maturity, Cyber Risk Analyser, Cyber Controls, Incident Response, SOC, Cyber Recovery, and Assurance Testing.

Want to learn more? Get in touch..

0203 8232 999

info@secrutiny.com

www.secrutiny.com