TAG Cyber Security Annual

2ND QUARTER 2022

CYBERWAR

A SPECIAL ISSUE

ARTICLES / OPINIONS / INTERVIEWS

WELCOME TO THE 2022 TAG CYBER SECURITY ANNUAL 2ND QUARTER EDITION

LESTER GOODMAN,
DIRECTOR OF CONTENT,
TAG CYBER

As I type these words in early April 2022, Vladimir Putin continues to bombard the cities and citizens of Ukraine in what is certainly the most important conflict in Europe since World War II.

And as people around the world watch the daily news with growing horror, the previously esoteric issue of cyberwarfare has emerged as a kitchen-table discussion topic, arguably on par with the nuclear and biological threat in its potential consequence to humans.

In this 2022 TAG Cybersecurity Annual— 2nd Quarter Edition, we tackle the topic of cyberwar from several different perspectives. On the one hand, we try to help readers understand how a cyberwarfare conflict might actually play out. This is necessary to bring cyberwar out from the pages of textbooks and onto the doorsteps of every citizen.

On the other hand, we try to offer dispassionate views of how cyberwar must be addressed by businesses, governments, citizens and technology providers. We do this in the voice of our expert TAG Cyber analysts—perhaps the most experienced assembly of experience and talent in cybersecurity in the world.

Be warned: This volume is uncomfortable reading. From our illustrated depiction of a feasible warfare scenario to Dr. Amoroso’s chilling argument that patterns predict that a global cyberwar will emerge by 2036, this volume will have you shifting in your seat.

But I hope you will spend time with this work. Read the feature articles and check out the interviews with the cybersecurity technology leaders included in the volume. Note that we asked each one to comment on cyberwarfare; it’s enlightening to see what they believe.

As always, we hope that you will benefit from our research—and we thank our Research as a Service (RaaS) customers in enterprise and our Content as a Service (CaaS) customers in the security vendor community for providing the support to enable our research and writing. It is through their kind support that we can offer this volume to readers for free.

Let’s all hope that by the time this volume hits the press in mid-April, tensions will have subsided and the Ukrainian people can return to their homes. Let’s hope that by the time you read these words, peace has returned to the region, and children can sleep safely with their families.

But regardless of what happens in Ukraine, the lessons learned from the conflict and their relationship to cybersecurity and cyberwarfare must not be ignored.

I hope you and your team will benefit from this volume, and let’s all hope for peace.

A SPECIAL ISSUE

CYBERWAR

AN INTERVIEW WITH COREY WHITE,
CO-FOUNDER & CEO, CYVATAR

MANAGING SECURITY FOR SMBs

The traditional view was that only large companies and agencies were targets of cyber threats. But this has since been replaced with the more accurate view that all organizations are targets. It's therefore sensible that managed security solutions have begun to emerge that meet the needs of this important small- and medium-sized business (SMB) segment.

Cyvatar offers fully managed security solutions with a complementary platform that includes many desirable features for SMBs. We were interested to gain some insight into how the solution would work in practice.

TAG Cyber: What is the major cyber risk challenge for SMBs?

CYVATAR: SMBs are a huge target because the cybersecurity industry doesn't care about them. The industry can't make money off smaller companies, so they tend to tailor their efforts toward larger companies. This leaves the SMBs to either figure it out themselves, or trust their local IT partner or managed service provider (MSP). SMBs are hit with large enterprise attacks, but don't have those large enterprise budgets or expertise.

TAG Cyber: How does the Cyvatar solution work?

CYVATAR: We're making cybersecurity "effortless and accessible" for our members. Most startups and SMBs do not have in-house security expertise, and they shouldn't. It's not cost effective to find and retain someone, and hope they have the expertise you need. And then, evaluating existing security products can take months. Finally, once inventory is acquired, you have to install, configure and maintain all products in-house. This is an inefficient process, even for larger companies. Cyvatar becomes an extension of your organization. We run your cybersecurity program, offering solutions—not just products, services and more alerts.

We identify your organization's security gaps, or we build a strategy from the ground-up, all within our proprietary platform before we sell you anything. We do not believe in selling solutions the member doesn't need. Our assessment gives us the insights we need to map out a security strategy for your organization based on your business goals and drivers. Do you need to become SOC 2 compliant? Do you plan to

Most startups and SMBs do not have in-house security expertise, and they shouldn't. It's not cost effective to find and retain someone, and hope they have the expertise you need.

hire aggressively? From there, Cyvatar and the member agree on a soluton roadmap. We then execute on our proprietary ICARM Methodology (installation, configuration, assessment, remediation and maintenance) and you watch it all happen within the platform. From GRC, to implementing security policies, your issues and remediation, Cyvatar does it all.

TAG Cyber: How do you deal with SMBs likely having little or no security staff to work with?

CYVATAR: It's our bread and butter. Cyvatar was founded on making cybersecurity accessible, achievable, and cost-effective for SMBs. We become that security staff or augment existing staff. It's simple. We hire the experts in our solution portfolio that have done it all, dozens of times. It makes no sense to hire internal staff that don't have the experience or expertise when you can get the people, process and tech from Cyvatar, bundled into a single monthly cost that's more cost-effective than a single full-time employee.

TAG Cyber: Tell us more about the services you include in your SMB offering.

CYVATAR: We have mapped all the compliance standards to understand what the basics are. Our solutions include: ITAM—IT asset management. This's important because you can't secure what you don't know you have. For example, how can you patch a system facing the internet if you don't know it exists and what software is running on it?

TVM—Threat and vulnerability management is a staple solution that every company needs. It includes continuous vulnerability scans, because approximately 50 new vulnerabilities come out per day. So, the reality is you can't scan weekly or monthly because you will miss something for sure. The scanning is just the identification you have to fix it in a timely manner. So, we partner with our members to create a patch management program. And we partner with the member again to fix the non-patch related vulnerabilities. We get our members to maintenance in 90 days or less.

CSM— Cloud SaaS management is a critical solution because it helps secure newer companies that do not have a firewall, or any infrastructure. It accesses cloud-based services for log review and alerting of SaaS solutions like Microsoft 365, AWS, Slack and G-Suite, to name a few.

SEM—Secure endpoint management is a core solution that all companies need. We use next gen AV that has the capability to block malware from executing. Most companies fail here because they use legacy AV and are not able to identify next gen malware. The second failure is that either they don't have the capability to block the malware; or, if they do, it's not configured. That's like having an amazing door lock on your house and never using it.

MSAT—Managed security awareness training is absolutely needed because human error is a huge threat to your organization, and if we can prevent an attack with user education, it's a huge win for everyone. No technical solution is needed. We offer phishing training along with all the usual attack scenario training. IdAM—identity & access management is another core solution needed by every organization because you should assume the hackers have your password—either from a previous breach or because it can easily be cracked. Since passwords are dead, there must be a second factor to protect user accounts.

TAG Cyber: Do you have any predictions about whether securing SMBs can play a role in future global cyberwars?

CYVATAR: Let's face it, most businesses are SMBs. What this means is that their attack surface is huge, and many of them don't have robust security programs. This makes them ripe for cyberattacks. SMBs are just low hanging fruit. So, if there's a major cyberwar, they will get hit first and may be used as a pathway to larger companies they may have access to, as in the Target breach.

A Cyber Security Class Somewhere in New Jersey:

"Do whut I say and yer bad emails will sleep with the phishes."