IT AND POWER IN PARTNERSHIPS

Because no one can do it alone!

KENJI MARTINEZ

IT and Power in Partnerships

Information Technology is always evolving, becoming more complex and requires more skill sets than one organization can hire. Cybersecurity has proven time over time again that even the largest of industries and companies fail to safeguard infrastructure. Failures in cybersecurity come from all different aspects, Network Administrator, Database Administrator, Information Security, Security Operations Center, Development Operations and more duties.

Understanding no one has the money to hire a full IT spectrum of talent

To have a wholistic solution that covers your infrastructure, there are many hats to wear. Besides your usual help desk personnel and subscriptions for anti-virus and application licensing, you will need many jobs that cover your vast and changing infrastructure. To manage your multiple sites interconnectivity, availability, failover and remote access is your Network Admin. To correct your queries and APIs is your Database Admin. To protect your infrastructure from outside intrusions, imposters and insider threats (even accidental via email compromise) is your Security Operation Center which is composed of at least 12 people (https://www.infosecurity-magazine.com/opinions/calculating-true-cost-soc/) to give your top to bottom resolution from detection to forensics and finally remediation.

Below are the costs of these employees plus some others that will be essential to your organizations success with keeping highly available and secure:

- Network Administrator- $70K/year
- Database Administrator- $75K/year
- Information Security Analyst- $81K/year
- IT Manager- $138K/year
- Chief Information Security Officer- $196K/year
- Security Operation Center- Employing 10-12 people at a minimum

When evaluating most businesses, these roles are far outside the costs of what an SMB would be able to afford. Even for the large companies that have a national or worldwide presence and more than 10's of thousands of employees will still outsource some of these specialties due to the cost of talent acquisition and cost of employment.

Areas of criticality

Cybersecurity is one of the nation's biggest shortages in employment right now. People in the information security field are making more at an entry level then some of the seasoned network admins. The skills required to start up teams like a Security Operation Centers is one piece, there is still SIEM, Security Information and Event Management, monitors are items required to be installed by compliances. There are many shapes and sizes to the SIEM that range from ready to deploy to customizable SIEMs that require technical specialties for programming SIEMs like Alien Vault and Splunk, two major industry SIEMs. Their job is to target your infrastructure's nuances and find ways to program the SIEM to detect and monitor the hardware and traffic while not causing notification fatigue.

They create custom dashboards and set severity levels to ensure the SOC team can accurately respond to meaningful notifications.

How do you choose a professional group or service?

In our operations, we follow the belief that one team can bring a solution but will need to do so in partnerships. This comes back to the concept of Batman. You have an educated individual that needs to strategically think about what tools are most impactful to your clients. Batman doesn't travel with a jackhammer on his back in case he needs to break through a wall. It is most important to notice he doesn't carry a firearm to check a box of looking official or a sign of justice. Some of the most powerful partners in our wheelhouse have proven time and again to be more valuable through times when management is not enough, and custom remediation or migrations come into play.

Telecom Consulting Group (TCG)

TCG has been a partner of ours for 2 years and have proven to be a great "outside the IT box" solution. TCG opens a channel of partners that have all been vetted and requalified throughout the year for best of breed solutions and customer service. Their channel provides solutions from Cybersecurity to internet (DSL, broadband, fiber, satellite, cellular and more) to Telecommunications (POTS, SIP, VOIP, cellular and more). The channel managers keep a high tough with their agents that ensure your requests are responded to in a timely fashion. We have found through the channel manager specific vendors that are white glove and fool proof when researching solutions.

What does this have to do with IT?

TCG bring a higher level of IT management. Their solutions help us as a Managed Security Service Provider by researching solutions through the industry's biggest and most reliable carriers. We have had may clients that still operate off DSL or unstable broadband lines. Two years ago, we decided that if we are going to be responsible for the infrastructure and remote access, why not be a SME, subject matter expert, on how their data is transported and how available we can make their infrastructure.

Examples of success:

- Finding more stable internet
- Lowering internet costs to reallocate to IT projects
- Finding failover internet sources to allow for remote site and sessions to be more available
- Costs reductions in telecom (usually 40% lower) to reallocate budget
- More secure telecommunication providers that can be managed within the network to meet compliances
- Finding vendors that fully manage the VOIP and internet solutions to allow our IT staff to focus on matters most relevant to their skillsets
- On demand engineering with low response times (usually 24 hours)

Channel only SMEs and their value

TCG has many vendors that only offer their solutions through channels, they do not sell direct (ex. AT&T has inhouse call centers, in store sales teams, indirect sales like BestBuy/ Target, authorized retailers that are privately owned, in home expert sales teams, outsourced call centers and channel sales such as TCG). The value we found in channel only solutions can be found in the competency of the SMEs. The SMEs are more than likely decades of experience in the field and have certifications or direct training to master the knowledge and understanding of why they are a solution and not a product.

Many of these SMEs are not afraid to also step back and tell you that they are not the proper solution and you should consult with another team that is better in the specific expertise you requested engineering or services for. In one case, we were working together with TCG's Vice President of National Sales, Kevin Zimmerman, who helped to partner up two vendors to create a cloud based VOIP and call center solutions that was driven by data analytics. Their team is driven by the solution and not profits, a true non-biased solution, rather than profits. TCG does not enforce "minimums" of participation to stay active and offer training with their channel partners to ensure you can stay abreast the new technologies and solutions that TCG has to offer.

Pax8

Pax8 is known for its ability to augments a business's Productivity, Infrastructure, Continuity and Security. From being the Microsoft and Microsoft partner channel, Pax8 too carries a special punch in the technical world. Pax8 employs its own Microsoft specialists that live, breathe and do Microsoft services. From technical knowledge to PAX8 Pro Services for email migrations to Azure infrastructure provisioning, Pax8 covers IT vendors backs when projects are too large for their engineering capabilities and bandwidths.

The Pax8 Experience

Pax8 is also a unique group that offers workshops and training to those that want to understand the newest cutting-edge technologies from Microsoft and tech companies that support Microsoft services and products. Everyone that becomes a partner is eligible to become a "Wingman", where a conference center is packed with supporting Microsoft vendors that have been vetted by the Pax8 crew. The Pax8 instructors also give materials and training of how to optimize and harden Microsoft services. The community in the room is unique since they are all IT vendors and open conversations to best practices and known issues with hot items. Last year's Pax8 Wingman training revolved around Microsoft 365 and the large changes to achieve a compliant and secure infrastructure for email services. They peeled the onion from how to qualify client's needs to each level of Office and Microsoft 365 subscription level to migration tips. After the migration tips were discussed, our "flight instructors" talked to the group about how Microsoft does not provide built in backups of data and *is not responsible for data loss.*

We quickly elevated the discussion about plugin services like DropSuite and Skykick to backup emails and Office Suite data (OneDrive and SharePoint). The last piece of the Microsoft Office and M365 services was how to use the new M365 tools to harden the environment from email compromise and enable audit logging to forensically protect your clients, or self, from insider threat and give the ability to responsibly report data theft when required by compliances like HIPAA.

The Pax8 Community

After becoming a new Pax8 Partner, you gain access to knowledge repositories and certified Microsoft help. From SMEs to engineers, there is few things Pax8 cannot handle. Pax8 is much like TCG where vendors are readily available to answer your questions and provide engineering support on demand. It is not common to find a powerhouse of both skill and partners that provide augmentation services and full engineering to implementation services. Pax8 knows its responsibility to its partners and vendors by answering only the questions they are certified to perform and knowing when to hand questions to the proper teams that are required to finish the job. They never disappoint when training their IT partners and do a great job of providing trainings in local areas to ensure most partners have easy access without the need for large travel accommodations.

Virtis US

Virtis US is an unrivaled next-gen and award-winning cybersecurity firm. Virtis started in New Zealand and currently protects multiple governments and medium to enterprise businesses. Virtis started with a unique Web Application & API Protection, WAAP, that uses the industries top computing and filtering under the close watch from an Artificial Intelligence, AI, driven Security Operation Center. For compliance and 24/7/365 abilities, Virtis employs a team of certified technicians around the world and locally based in the United States as well.

What Makes Virtis Stand Out from Other Cybersecurity Firms?

In the age of technology, no one can get a handle on what creates a secure environment. Amazon, CapitolOne, Target, The Department of Defense and more have been successfully infiltrated. Virtis has found a way to mitigate breaches and data loss through controlling the traffic in and out of the infrastructure and endpoints. Besides the WAAP, they have now launched a critical tool to working remote and even hardening the end point protection. When any firm goes through a vulnerability scan there are lists of exposures that range from critical to minor. Some firms can be found to have 50 vulnerabilities, which in my experience is low, and others can be in the 150-200 range, which is most common. Virtis can protect against ALL your known vulnerabilities while you go through the remediation process. The greatest part of the partnership, we can remediate at our own pace to not leave more exposures behind while trying to rush critical patches to the known vulnerabilities. If vulnerabilities are identified, the current remediation time stands around 6 months without a WAAP.

- Guarantee to protect 100% against all known vulnerabilities (and it is in the contract)
- Meets compliances for larger companies that must only use resources 100% operated in the United States
- No hardware is required to use the WAAP and it can be deployed from minutes to a couple hours depending on current infrastructure (on premise and cloud capable!)
- Removes risk from using old and outdated applications that are no longer supported from its developers
- Removes expensive vulnerability assessments from third parties that can be reallocated to protecting and remediation
- Have been proven to immediately work against active breaches
- Have scalable, high availability and hardened infrastructure to ensure they can mitigate any threats against your business
- Only large enterprises can afford the Web Application Firewall, WAF, and SOC maturity that Virtis carries. On a subscription cost, Virtis costs around the same as most WAF subscriptions but offer the WAAP solution to combat against more sophisticated exploits.
- Virtis is a layered security approach that does not open back door vulnerabilities to your existing security posture. They are placed in front of your infrastructure rather than inside it.

What Else Can Virtis Do?

Virtis also provides other remarkable services such as micro segmentation, a very meticulous and strategic way to slow down and eliminate cyber breaches. They deploy into your network to watch and understand the paths of how your network communicates inside of itself. Once they can diagram out the workflows and assets, their teams set boundaries to segment network assets and machines from communicating with one another if it is deemed not necessary to accomplish their roles in data transport. This rule is like the NIST 800-171 DFARS control of least privilege, a user will only be granted access to a system and the access within the system is at its bare minimum to allow the user to perform their work, except we can controlling the systems much like you would a user.

OneTRUST, is Virtis's newest and greatest end point protection that again is an industry leader in gaining secure connections to your infrastructure. Beyond the security of a VPN, OneTRUST is added to your businesses applications that allow remote access. At any time, a user can go to your login portal and a secured session starts and credentials are verified with the domain controllers to allow access. OneTRUST verifies the hardware (trusted devices) and uses a biometric data collection, a step above MFA, to create a profile for each user. Each user can be recorded from their typing speeds, mouse jitter, location and known hardware. If users are logged in from separate locations within the same session, OneTRUST will block the rogue access even if the credentials are correct. OneTRUST also allows management from the portal to set group policies. User passwords are forced to abide by a minimum-security standard and can disable autofill abilities from the browsers. On top of minimum standards for passwords, OneTRUST provides a dark web scan of user credentials to ensure the password is not compromised and at a minimum alert the user while logging in but can be set to force an immediate password change.

The installations do not require hardware and can be configured within hours, meaning vulnerabilities and breaches can be stopped same day.

Hook Security- PsySec Training

Hook Security is redeveloping the concept of Cybersecurity Awareness Testing and Training. Organizations commonly underrate importance of Cybersecurity Awareness Testing and Training. Today's standard for most California based companies is to get the sexual harassment training deployed as soon as onboarding as the start of each calendar year. Many products are available and offer continuous training but fail to engage and test the end users that risk accept vulnerabilities through rogue applications, compromised emails and phishing attempts. Organizations and IT vendors also forget that as part of a client's compliance, all vendors must follow the compliance and security flow downs (client to IT vendor to software to maintenance vendor). Hook Security though of not just a modern-day solution but also meets the most common compliance mandates for cybersecurity frameworks. With a NIST SP 800-171 compliance, they will be a viable solution to deploy for clients that follow compliances such as PCI, HIPAA, FINRA, NIST SP 800-171, and CMMC Level 3 (currently in preparedness for and awaiting accreditation) and below.

IT Vendors and Cybersecurity Awareness Testing and Training

Notably, many IT vendors will choose a subscription and fail to deploy the software to customers even when it is listed as part of the standard services. Much of this comes from not having enough bandwidth to learn and deploy the subscription to the users. Hook has created a model that is a full solution when it comes to deployment. Since Hook is the owner, developer and expert in the software they take ownership of deployment to ensure IT vendors are not help responsible to learn new systems. Hook provides a customer questionnaire of 15 items in order to deploy. All users are given a live person from Hook's customer support team should issues arise, given IT vendors a break from responsibilities of managing something they do not have control over.

Why PsySec over traditional Cybersecurity Awareness Testing and Training?

Hook Security takes a different approach to training and security testing. The continuous testing and training are interactive with real everyday threats such as personal emails (Netflix, Disney+ and Bank of America impersonations) to business emails (COVID Healthcare enrollment, ADP and more), challenging users with up today's most common phishing attempts. This training also teaches pattern recognition along with (brain) muscle memory of how to properly vet emails and compromises.

> **"20,373: Number of complaints the FBI received last year involving business email compromise (BEC) attacks**
>
> BEC fraud resulted in losses of over $1.2 billion last year and continues to remain one of the most prolific and fastest-growing crime categories." – Tech Beacon

The program is a cut above by identifying struggling employees. Hook has created an intensive training program, forcing those who fail 2 or more trainings into a deeper set of training. This is a great tool that is part of the subscription costs. This differentiates those "checking the compliance box" vs those who want to leverage the employees paid time into defending the corporate's assets and reputation. This process ensures that those who are not "technically savvy" can receive a more insightful and custom tuned training to become a cyber guardian.

Vendor Integrity and ingenuity

Hook Security plugs into most active directories. The software syncs and onboards new users as well as decommissions terminated users. This sync helps HR and IT automate the onboarding and offboarding process. At the end of the day, are you most interested in saying you deployed the training or that your team was able to identify and mitigate this year's attempts to phish and compromise your business?

How do you manage them to ensure they are managing you?

It is best practice to hold quarterly or biannual meeting with your reoccurring services vendors to ensure you are properly managing your vendors. Each vendor should be able to report project statuses, be presenting objectives and recommending new milestones. For those that want to check the proactive management, see the previous article "How to know when to fire your IT company". A series of questions are outlined to help non-technical manager to receive quality answers from their IT vendors to ensure the main backup systems and securities are in place and being managed.

Here is a short guide to what should be strictly governed quarterly:

- Backups
  - Completion reports of nightly backups
  - Test restoral of backups for data integrity
- Security
- Have patches, OS updates and firmware been applied to all machines and network devices?
    - This should be within 2 versions at a minimum
- If you have SIEM monitors-
    - Request a report of positive threats and check their notification time vs their remediation time.
  - Getting an overview of the architecture to understand what is covered in the monitoring. Ex. Network at corporate office, Office 365, EDR on workstations outside of corporate network and etc.

- Billing
  - Request a detailed bill of tickets that were out of scope. Run the "out of scope" services against the contract's MSA/ services agreement, which you can make into a simple matrix, to validate the "in and out of scope services".
- A list of open tickets and projects
  - The list should detail ticket creation dates that can be checked against the SLA's issued from your vendors MSA/ services agreement. You can tell if they are having performance issues or if your projects are not being properly project managed. This allows for your oversight to ensure your compliance deadlines are being met.
- Reviewing Compliance and Security
  - Keeping a running list of vendors and subscriptions
    - Reviewing that all software and vendors that have network access are certified or attested to be compliant with your organization's compliance.

If you find yourself overwhelmed and require a professional IT consultant to guide your organization to a qualified IT vendor or wish to get second opinions about IT initiatives, reach out to Oversight IT Consulting for an unbiased and vendor-agnostic approach.

Kenji Martinez
Founder and CEO
Kenji@OversightIT.com