Pacific Global Security Group

The Value of a Virtual CISO in Small/Mid Tier Businesses.

Who is Pacific Global Security Group (Pac-Sec)?

- Pacific Global Security Group is a cyber security company headquartered in Honolulu, Hawaii. It is staffed by a team of tier one cyber security specialists with global experience, dedicated to providing secure, trusted, and integrated cyber protection services to government agencies and businesses alike. Pacific Global Security Group offers a complete portfolio of cyber security solutions with all our work being underpinned by industry leading intelligence, research and development (R&D).
- Comprised of former Big4, DarkMatter, and Military security professionals. Pacific Global Security Group's team has extensive cybersecurity experience across a wide range of industries from government to critical infrastructure as well as the deep understanding of advanced secure technologies. Pacific Global Security Group can assist you with selecting, designing, and the implementation of the right solutions to reach your cybersecurity, risk and privacy goals. We Strive to raise the bar for small business cybersecurity capabilities.
- Our mission is to safeguard US Government infrastructure and its assets from both internal and external attacks and enable mission continuity for our war fighters. Also, to improve the cyber-security posture from ground zero and form a better cybersecurity eco-system for all. At Pac-Sec, we're committed to exceed the governments expectations and ensure complete satisfaction. Our team of experienced technical managers work diligently together with the government to ensure that our quality of services is unparalleled in technical, compliance and all performance metrics are met. We follow industry best practices and use the very best of experts who have technology market Insights in all aspects of cybersecurity.

Did you know: 43% of all breaches occurred in Small/Mid size businesses? - 2019 Verizon Breach Report

- Information Security most likely doesn't drive your business, but it will help keep you in business.
- Most small/medium and even big businesses and Government can't justify having a full time Information Security team on staff.
- Mid market businesses (Primes) run the same applications, and have similar infrastructure as larger corporations, just at a smaller scale.
- With corporate breaches constantly in the news, the specter of being the next "Pwned Company" looms large in the boardroom.
- Mid tier businesses are also accountable for the same regulatory controls and reviews as their larger counterparts.

The Supply Chain to larger businesses

- According to Chamber of Commers, there are 30.2 million small businesses operating in the United States.
- Importantly, these companies also serve, supply and partner with individuals and larger organizations. Not having the resources to deploy complex security stacks makes them easier targets.
- The attention around cybersecurity breaches is only going to grow thanks to the new changes to global privacy regulations.

One Breach or Ransomware event will likely cost you more than several years worth of Cyber Security Guidance!

Drivers for Small to Midsize Business Cyber Security Requirements

- Government agencies and business partners requires validation that you are protecting their data. (CMMC)
- Data Breach - loss of corporate intellectual property, customer data, employee data, or business partner data.
- Ransomware Event – systems are down, and you're are locked out.
- Regulatory Requirement – your industry requires periodic validation of your security controls.
- Client requires validation that you are protecting their data.
- Insurance company requires validation of Cyber Due Diligence.
- Mergers & Acquisitions – acquiring company requires validation of Cyber Due Diligence.

Common Risk issues across Industries.

Business is business is business… Much of what a CISO can provide is common across business scale, and across industry verticals. The audit firms make a killing in rinse and repeat audit reports. Their findings are almost identical in every company they assess.

- Lack of appropriate Security Policy Framework
- Failure to comply with documentation that DOES exist
- Absence of periodic review and update based on current environment

- Privileged Access Issues
- No least privilege policy – too many people with privileged access
- No periodic review / attestation of privileges
- Failed regulatory compliance for FedRAMP/SOX/HIPAA/PCI, etc…

- Vulnerability and Patch Life Cycle
- Lack of policy/standards to guide/enforce appropriate patching
- No regular vulnerability assessments across complete network
- Windows systems OS somewhat patched, but other platforms missed
- Middleware and application space completely missed

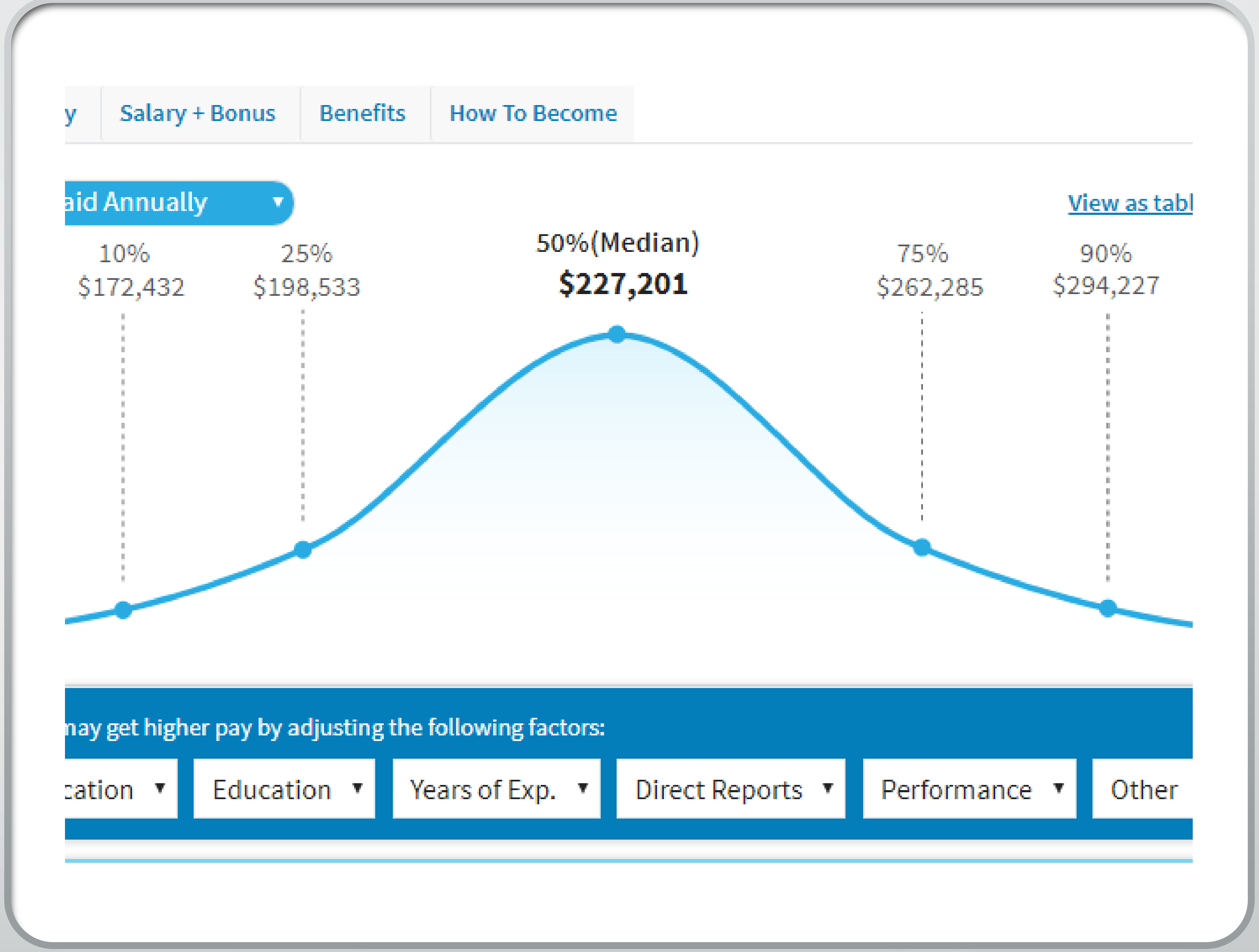
- Monitoring, Reporting, and Alerting Issues
- Either no monitoring is in place, critical assets are not all monitored
- No understanding of "use cases" for alerting/reporting
- No regular review of alerts/reports

- Ongoing Posture Metrics and Trending
- Security metrics are not collected/reviewed
- No "posture" visibility to the corporate executive
- No baseline established for comparisons
- No weekly/quarterly trends to gauge improvements

- Security Awareness
- No regular Security Awareness program in place
- "Dated" annual presentation via PowerPoint or email
- No proper attestation as to employee understanding

Salary Expectations of the (fulltime) CISO

- As of today (2020) a typical company in the US can expect to pay their CISO between $198k and $262k per year.
- Not only is this out of reach for most Government entities, but the amount of Cyber Security governance required between an enterprise and an SMB differs.



https://www.salary.com/research/salary/benchmark/chief-information-security-officer-salary

Introducing the Virtual CISO

A Virtual CISO, or vCISO is an outsourced security practitioner or provider who offers their time and insight to an organization on an ongoing basis, usually part-time and remotely.

Variations on the Virtual CISO theme

Virtual CISO:

- Certified CISO with enterprise experience who works mostly remote and provides services to SMB/SME on an hourly basis, typically a 20-50 hours a month distributed throughout the month.

Interim CISO:

- Certified CISO with enterprise experience who swoops into a company to temporarily fill the void left by an outgoing CISO while the company has time to search for their Unicorn.

CISO Advisor:

- Certified CISO with enterprise experience who shadows an existing CISO to either augment their Governance team or provide the existing CISO advice and guidance on various governance tasks.

The Small to Midsize Business appetite for a CISO role.

- Most mid market businesses (250-2500 seats) cannot afford the expected salary of today's CISO, however their risks are the same.
- Midsize Businesses run the same applications, and have similar infrastructure as larger corporations, just at a smaller scale.
- With Corporate Breach constantly in the news, the specter of being the next "HVAC Company" looms large in the boardroom.
- Midsize businesses are also accountable for the same regulatory controls and reviews as their larger counterparts.

Virtual CISO Services

- Security Policy Framework
- Review and update Information Security Policy
- Review and update Information Security Standards
- Review and Update Information Security Procedures

- Security Awareness
- Review and update/create Security Awareness program
- Roll-out Awareness program to employees and manage

- Security Liaison with Executive Council, Auditors
- Manage communications with board of directors
- Manage internal and external information security audits

- Privileged Access Management
- Conduct privileged access discovery
- Clean up excessive privileged accounts
- Develop periodic review process/ attestation of privileges
- Validate compliance for SOX/HIPAA/PCI, etc…

- Vulnerability and Patch Life Cycle
- Implement regular vulnerability assessment program
- Review and update patch management process as per results of vuln scans

- Monitoring, Reporting, and Alerting Issues
- Review current log event management
- Update/Create log/event management infrastructure
- Develop use cases based on business requirements
- Create regular review of alerts/reports

- Ongoing Posture Metrics and Trending
- Collect, document, review security metrics
- Develop dashboards and baselines for information security
- Provide executive reporting on Security Posture

- Breach/Incident Response Plan
- Review/update Breach Response plan
- Create communications templates
- Conduct Tabletop exercises with Business and IT

- Secure Software Development Lifecycle
- Work with Project Management Team to provide Information Security guidance on new projects
- Implement Secure Code reviews/assessments/scanning

- 3rd party assessments
- Review security controls of 3rd party infrastructure/software/service providers

You can't Govern what doesn't Exist.

- It's all well and good to assess and document a company's security stance, but if there are no means to implement and manage, and monitor security controls on an ongoing basis, then you will have no chance of long-term success.
- For a Virtual CISO implementation to succeed, there must be an operational security function in place as well.
    - Convert/train existing company IT staff in Information Security Operations.
    - Hire 3rd party IT Security company to manage operations.
    - Contract your own staff to provide IT operations.

Holistic service…

- One person cannot be or should not be expected to be good at all things.
- A Virtual CISO (Or any CISO for that matter) has pool of talented resources at their avail to deliver various aspects of their Cyber Security Program.
- These would include, but are not limited to:
  - Penetration testers
  - Security Operations analysts
  - Security Awareness Trainers
  - Technical Document Writers

Security Processes to Implement

There are several processes and procedures that *must* take place in every organization, for a Cyber Security Program to succeed

- Identity Management
- Asset Management
- Security Awareness
- Change Management
- Incident/Breach Management
- Patch/Vulnerability Management
- Secure Software Development
- Backups / Restore / Business Continuity
- Vendor and 3rd party Management

First 30 days of vCISO Engagement.

In the first 30 days, the **"CISO for Hire"** would conduct an industry standard framework maturity assessment and gaps analysis across all the cyber security domains.

- This assessment serves multiple purposes.
  - First, it introduces the new CISO to the various stakeholders across the company.
  - Secondly it provides the business with a tangible graphical posture assessment.
  - Thirdly it identifies opportunities for additional governance and operational contracts.
  - Finally, it provides a quick method of establishing trust, credibility, and authority.

Next 60 days.

Once the Maturity Assessment and Gaps Analysis has been completed, the Roadmap to compliance can start to be developed:

- Cyber Security Policy Framework
- Identity and Access Management
- Asset Management
- Vulnerability Management
- Patch Management
- Incident / Breach Management
- Business Continuity…

Relationship building by requesting a cadence of short status meetings with the various corporate stakeholders listed above. At the end of the first managed quarter, an executive report must be produced, documenting progress to date, proposed compliance roadmap, risks uncovered, and ultimately a posture heat map backed up with quarterly metrics from all current protective/detective controls.

The Follow on…

At this point, much of the role should be ready for a rinse-and-repeat.

- Continue Policy framework development.
- Assess current gaps between policy and operational practices – provide guidance.

Initiate next quarterly review of privileged access across all critical platforms / applications

- This is a good time to start the discussion of bringing on a Privileged Access Management tool (CyberArk) to facilitate least privilege policy.

Provide governance and guidance over the Monitoring/Reporting/Alerting process.

- This is a good time to start the discussion on Managed SIEM if the client does not have one, or even if they are loosely running one in-house.

The Follow on…

Initiate regular employee engagement emails on Security Awareness issues

- At minimum monthly (but better weekly) send out a short, relevant, and to the point, Awareness Bulletin via email to all employees.
- This is a good opportunity to engage services to develop a comprehensive Awareness program.
- This is also a good opportunity to conduct a phishing exercise.

Adoption of Governance:

- Continue the regular cadence of meeting and understanding the roles and goals of the various business stakeholders.

Pacific Global Security Group

Thank you