A Day in the Life of a Cyber Security Pro

ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Infobrief

Written by David Monahan

Prepared for Bay Dynamics

April 2017

IT & DATA MANAGEMENT RESEARCH • INDUSTRY ANALYSIS • CONSULTING

Executive Summary

EMA surveyed over 400 individual contributors and management personnel working in cyber security, fraud, risk, and compliance to understand what they do to support operations on a daily basis. Interestingly, lack of budget was only a minor part of their frustrations. The lack of people was a top concern, but that is really only a symptom of a much larger problem.

The research identified a façade of program maturity, creating significant levels of frustration and stress with the operations teams, more so on the individual contributors than the management. From the data, it appears that each level of security operations is buffering the level above them from many of the stress-related issues to appear more efficient than they really are, which is a key cause of the overinflated opinion of security program maturity.

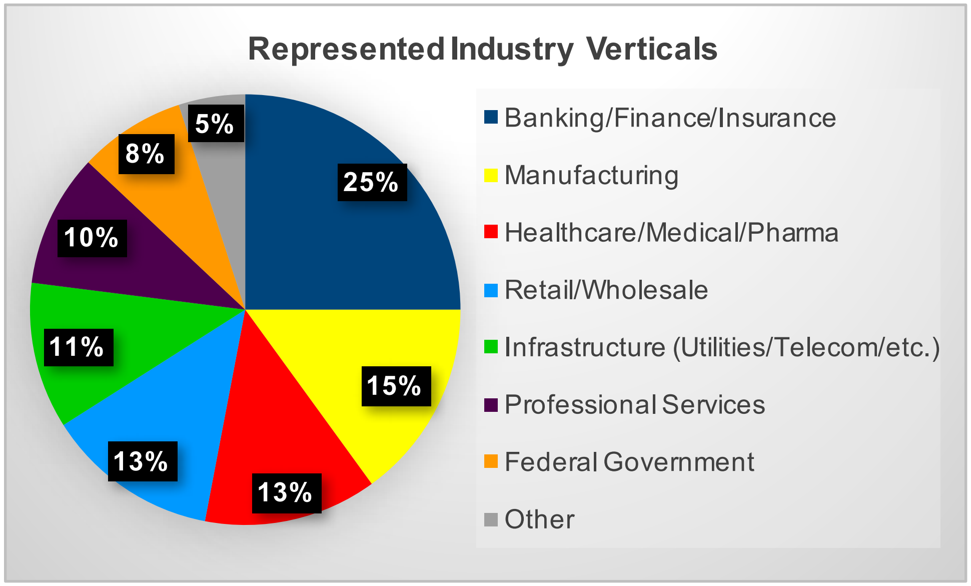
Demographics

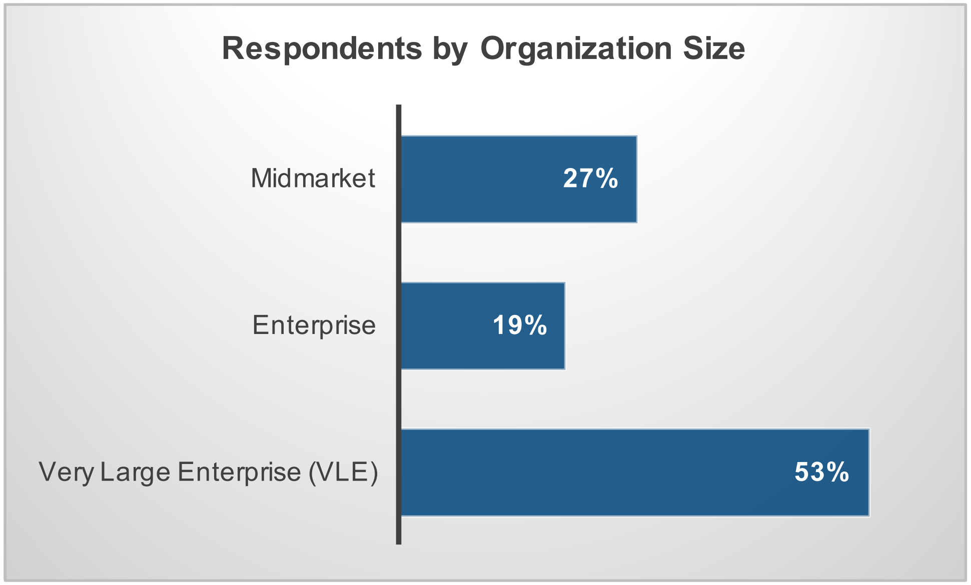
Research participants were located in North America.

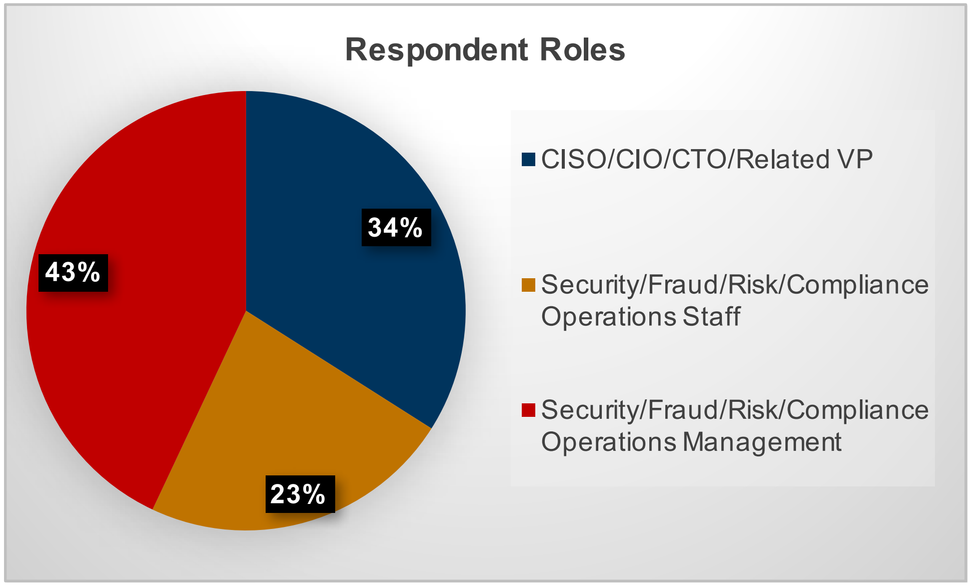
Research respondents came from multiple security, fraud, risk, and compliance organizations. Their roles represented each level of operations, from c-level and vice presidents down to the front line operations staff.

The target company size was mid-market and above, with the largest respondent pool coming from very large enterprises (20,000 personnel and greater).

Each of these is a key factor in the research to ensure that viewpoints are all represented. Often, research finds that different industries and different levels of personnel have varied views on what is really going on in their organizations. Staffs shield their management, who in turn buffer their executive team from problems. This dual protection creates a much "rosier" picture at the top of the pyramid.







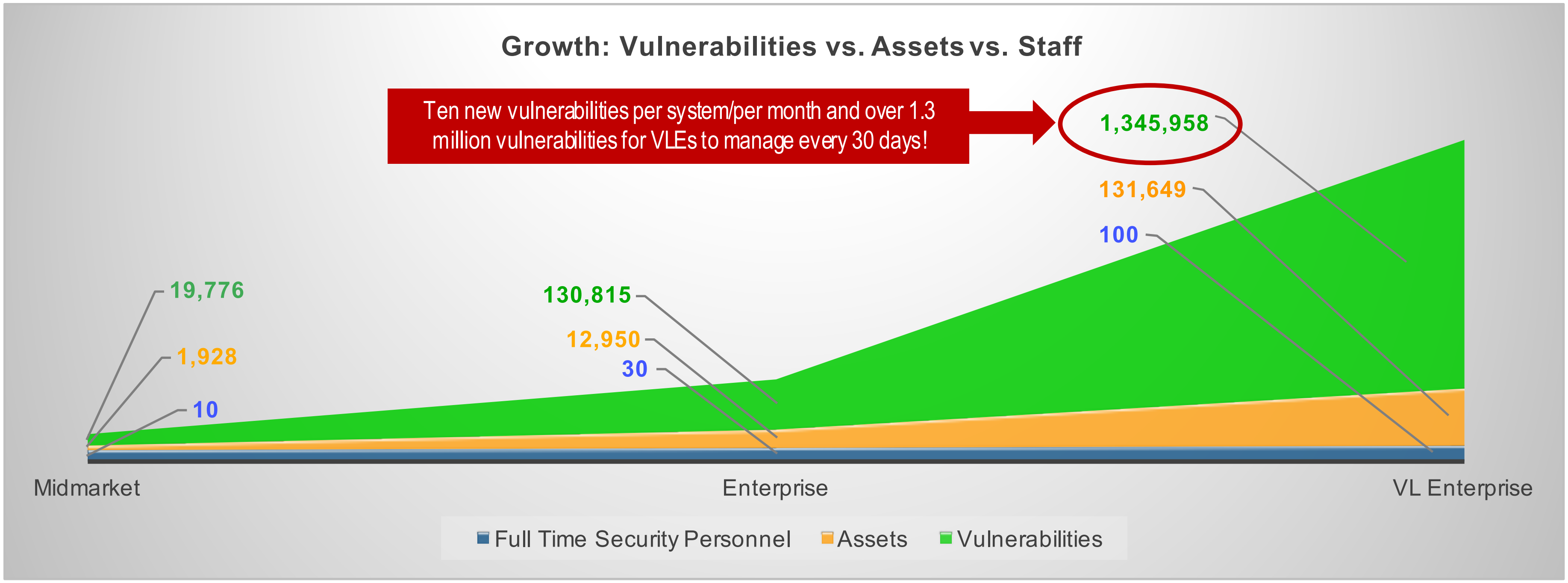
Too Many Vulnerabilities

Respondents identified that they have to deal with a large number of vulnerabilities in their organizations. On average, ten vulnerabilities exist per system.

Though midmarket organizations have fewer systems than enterprises and very large enterprises (VLE), they also have proportionately smaller budgets and teams. This makes them generally less sophisticated when dealing with the deluge of vulnerabilities and patching they are faced with, creating a larger burden for administrative and security staff.

Respondents from VLEs indicated that they are managing over one million vulnerabilities across all systems in their environments at any given time.

Though a majority of these vulnerabilities are duplicates across common operating system platforms and widely-distributed applications, not all systems can be treated the same depending on what function they play in the environment. While user endpoints may be patched virtually on-demand, physical or virtual production servers must be scheduled to ensure there are no business interruptions. Ensuring all vulnerabilities are appropriately managed and mitigated causes a significant amount of pressure on the staff.



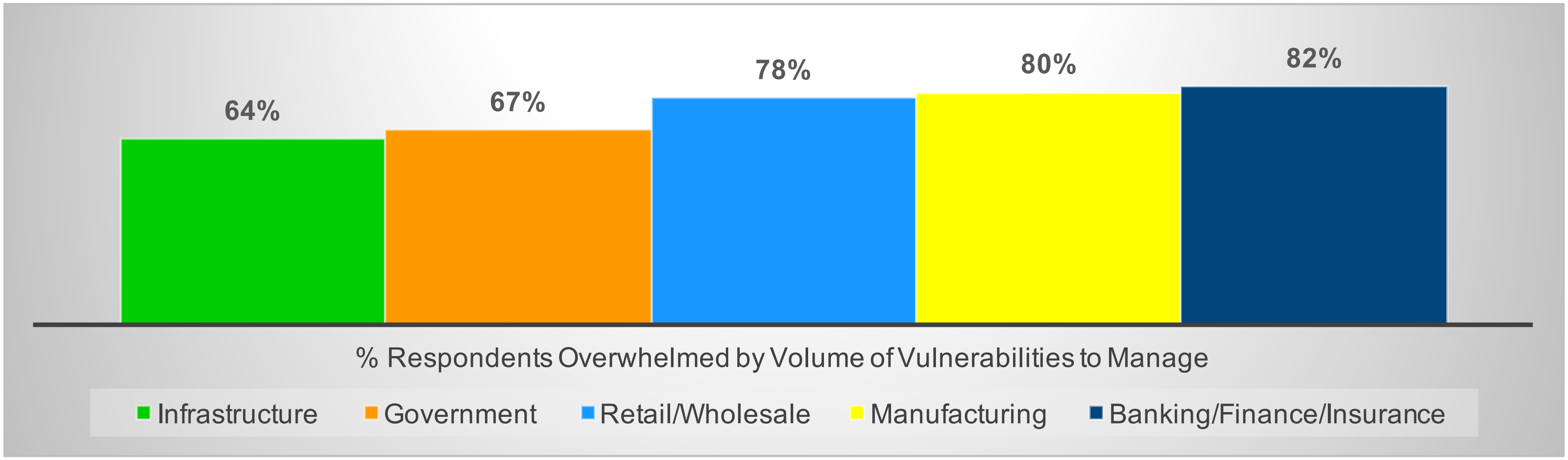
Staff is Overwhelmed by Vulnerabilities

74% of security teams stated they were overwhelmed by the volume of vulnerability maintenance work assigned to them. This is a tricky situation. The research revealed much of why they are overwhelmed and is discussed later in the report.

It is clear from the industry vertical information that having a lot of money is not always a good thing. Though the Banking/Finance/Insurance industries have the highest budgets in the commercial sectors, their security staff are also the most overwhelmed. Aside from Government, these industries often have the largest infrastructure to maintain.

Manufacturing is becoming more stressed due to automation systems and the embedded Industrial IoT systems. The systems are often hard to impossible to patch and must have mitigating or compensating controls put into place to protect them.

74% of security teams stated they were overwhelmed by the volume of vulnerability maintenance work assigned to them.

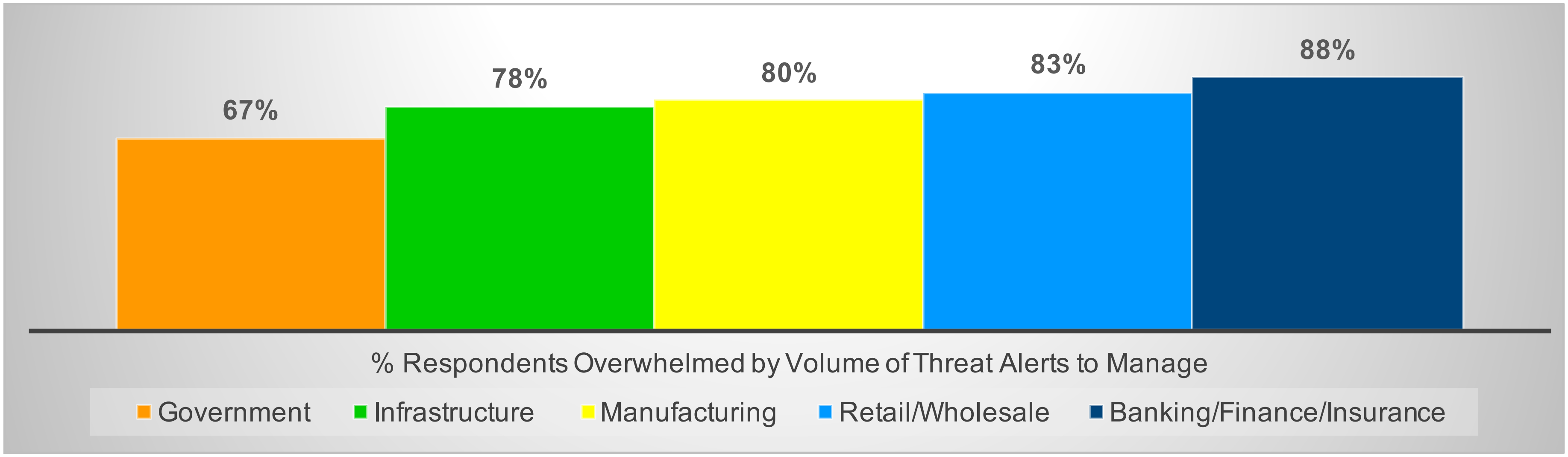


Staff is Overwhelmed by Threat Alerts

By once again viewing the data by industry vertical, it is clear that the Banking/Finance/Insurance vertical is still at the top of the stress pyramid and within six points of the levels identified for vulnerabilities. Manufacturing and Government indicated the same levels of frustration in both areas.

While Retail/Wholesale rose by five points, infrastructure rose by 18 points. Infrastructure verticals increased deployment and dependence in connected IoT systems, such as smart meters and remote grid management SCADA systems. This dependence made them a greater target for hackers ranging in activity from casual hacktivists to determined nation state actors.

79% of security teams stated they were overwhelmed by the volume of threat alerts. This is closely in synch with the levels identified with vulnerabilities.



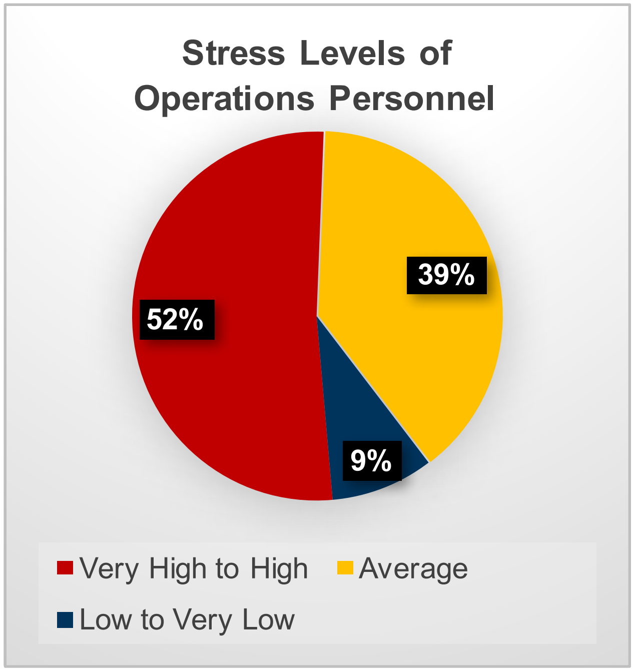
Stress is Building

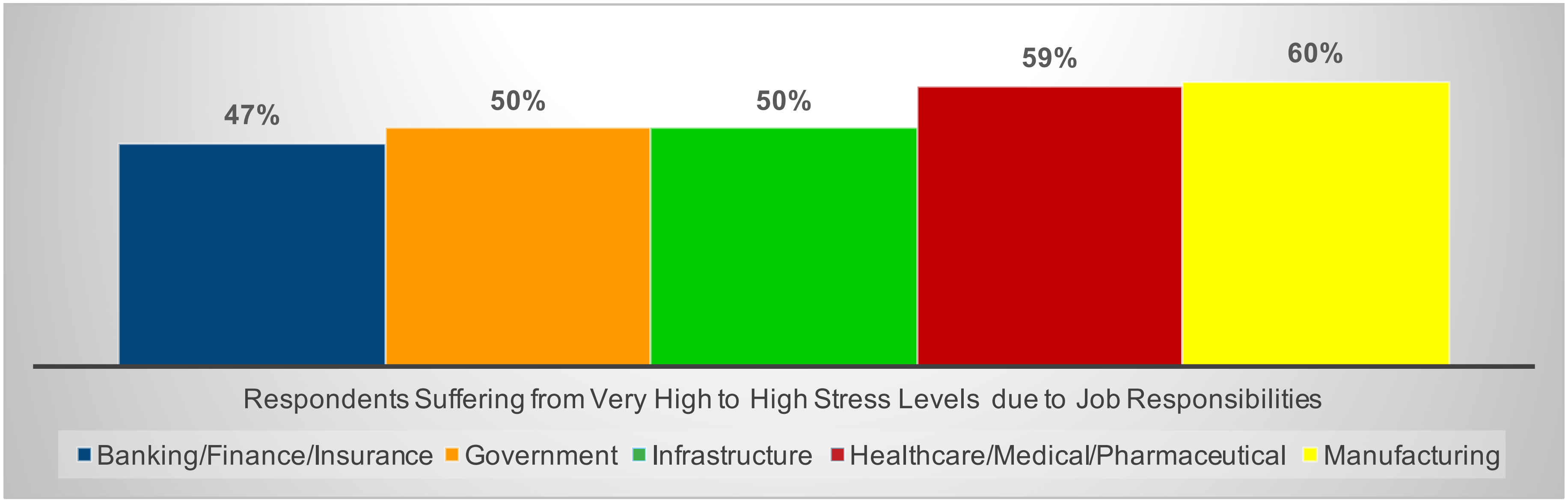
The pie chart to the right indicates the overall stress levels experienced by operations personnel. Significant demands are placed on all levels of security operations to do more, faster. The increase in productivity requires some form of change to increase volumes by either applying more resources or greater efficiencies.

Looking at the column chart below, it is interesting to note that by their own admission, Manufacturing organizations are not the most "overwhelmed," but they came out on top for stress. This is most likely caused by the fact that Manufacturing organizations are generally less prepared to fight a cyber war than their Financial and Government counterparts. They are also a high-value target for hacking groups looking for data to sell and nation states looking to improve their manufacturing capabilities.

Medical organizations feel the pressure as well. Over the last few years, HIPAA regulators have become more strict and the pressure from hackers increased since personal health records (PHR) prices are rising on the dark web.

Infrastructure and Government are both major targets of nation state groups; not only for their information, but also for control of resources. Attacks on utilities climbed steadily over the last ten years.





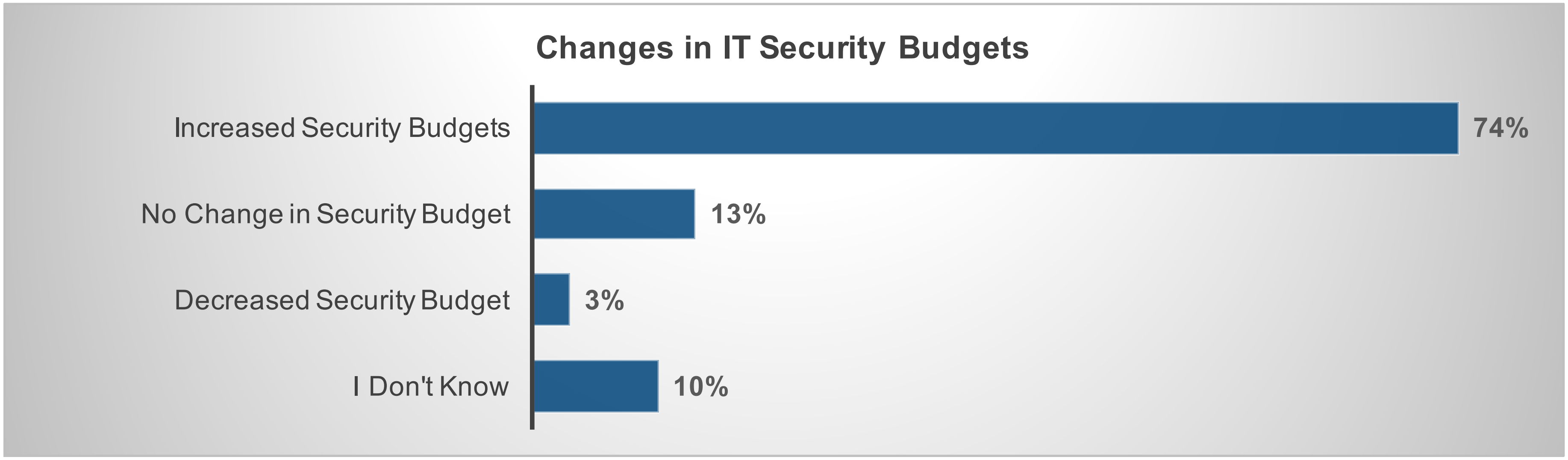
Stress Drivers

The first thing the research indicated was that budget decreases for security were not a stress driver. In fact, 74% of organizations reported a budget increase, while only 3% indicated the opposite. The average budget increase was approximately 12%, which is healthy considering increasing security budgets are a three-year trend.

Aside from budgets, security teams had plenty to worry about.

The first issue concerns the vulnerability management program. Nearly 80% of respondents said their organization's patching approval process was significantly manual. This included emails, spreadsheets, and other electronic documents for tracking and approval. With the volumes of patching that have to be reviewed, these labor-intensive manual steps drive high inefficiencies and stress. Given the level of program maturity respondents indicated existed in their vulnerability management programs, this was very surprising.

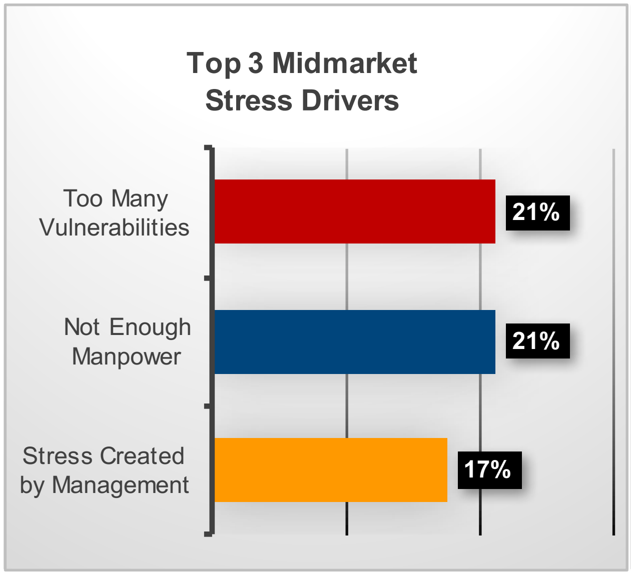
79% of respondents said their organization's patching approval process was significantly manual.



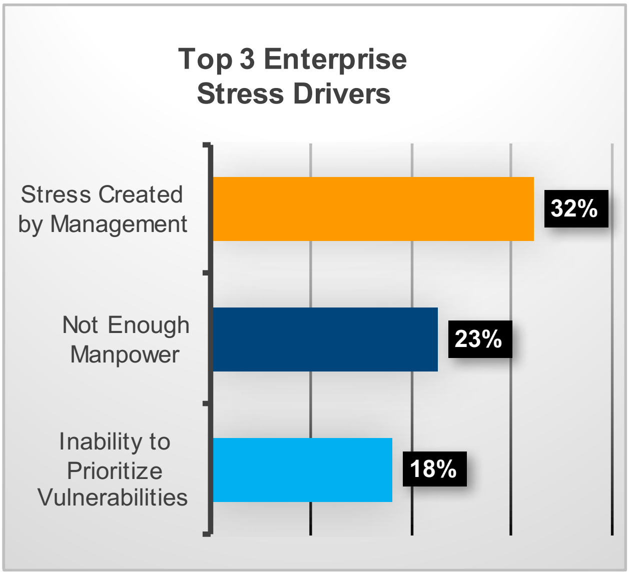
Stress Drivers by Organization Size

Respondents are creating a security façade around their security program maturity. This could be a natural extension of what they are conveying to their upper management. Management expectations seem to significantly drive workplace stress. At 21%, “stress created by management” tied for second-highest stress driver with “too many vulnerabilities,” and fell one point short of “not enough manpower.”

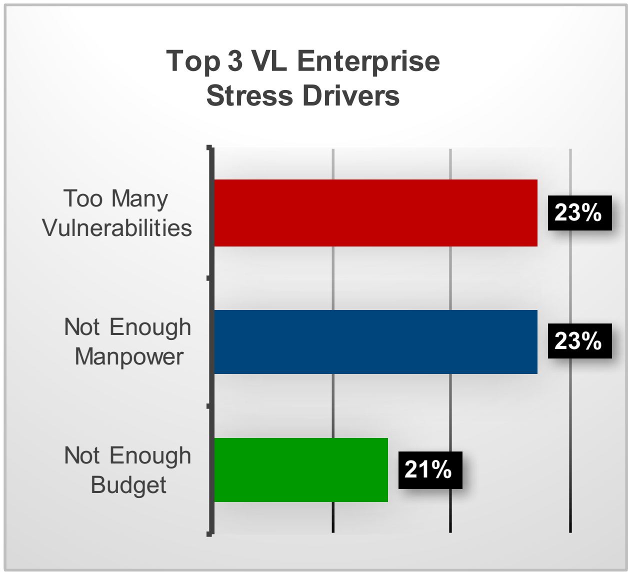
Looking across organization size, ”stress created by management” was a top three factor for both midmarket and enterprise-level organizations, but dropped out of the top three drivers for VLE. It was interesting to see that VL enterprises identified “not enough budget” as an issue despite the increasing budget trends. 62% of VLEs indicated they had budget increases and only 14% indicated budget decreases. Granted, everyone can always use more budget, but the VLEs tend to have greater proportionate budgets on IT and security to begin with.



Top 3 Midmarket Stress Drivers



Top 3 Enterprise Stress Drivers



Top 3 VL Enterprise Stress Drivers

Stress Drivers: Alert Misprioritization

While severity of alerts should be a key indicator of how both vulnerabilities and threats should be prioritized for action by operations, it is not the only factor and should not be considered the primary indicator unless the prioritization algorithm has sufficient context within its framework. Security operations teams are highly dependent on severity to classify alerts, but alerting systems like security incident and event management (SIEM) systems are most often not imbued with the data needed to make a proper judgement. This creates a situation where too many alerts are created, with the highest priority then requiring additional work by analysts to make a proper reprioritization.

Respondents indicated they have to manually reprioritize over half of the threat alerts they receive. Not only is this indicative of a less mature program because it drives more work and delays resolution of the truly high priority alerts, it significantly raises stress and the feelings of being overwhelmed (NOTE: at a minimum, frontline analysts should be able to rely on system prioritization for well over 75% of their alerts. In a well-honed environment, manual prioritization should be below 5%).

The underlying cause of this rework is a lack of context. Areas of additional context that should be considered before prioritizing threat alerts include financial impact if an asset at risk was compromised, asset value, associated vulnerabilities that would enable the threat to succeed and, in the case of insider threats, qualification from application owners if usual behavior was business-justified.

68% of respondent organizations prioritize vulnerabilities based on their severity.

58% of respondent organizations prioritize vulnerabilities based on the severity of the identified threat(s).

52% of threat alerts are improperly prioritized by systems and must be manually reprioritized.

Sneak Peak:
Self-rated Vulnerability Management Program = Security Façade

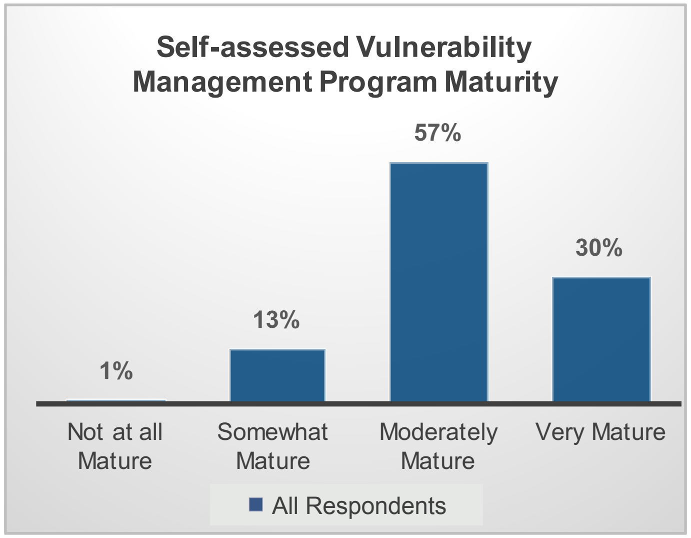
There is a significant issue with the self-ratings respondents provided about their security program maturity. Before asking to self-assess, participants were provided guidelines on what constituted a level of maturity. "Moderately mature" and "very mature" programs should have significant levels of automation across their operation's management processes.

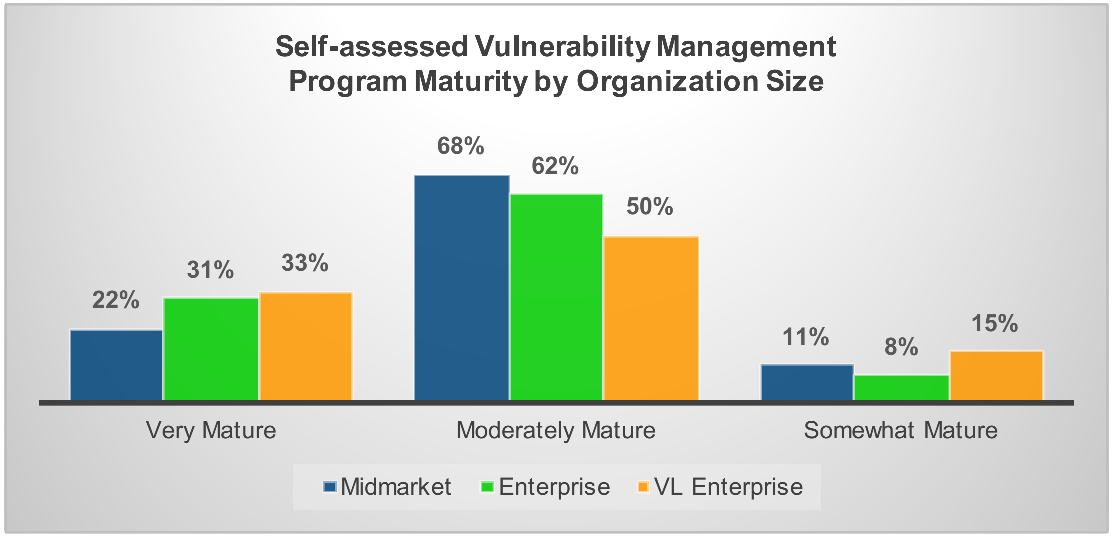
Though 87% of organizations indicated they had a "very mature" to "moderately mature" patching process, 79% indicated they are using emails and spreadsheets during the patching approval process. These tools require significant manual intervention and management, can be highly error prone, and are not automated and not part of a mature program. This indicates that respondents had an over-inflated opinion of their programs.

The breakout of perceived program maturity by organization size is also visible. Very large enterprises had the highest average opinion of their capabilities and though many should have "very mature" processes, it was clear that many did not reach that level of performance. That load, combined with the large volume of threat alerts, would definitely increase stress.

Either management expectations are too high or each level of the security management chain is insulating their higher-ups from the challenges. It is most likely a combination of both. Though to some degree everyone hides a level of difficulty in their roles from their upper management because they want to look good for their managers, it seems to be taking a toll in security.

Hiding the difficulties would lead upper levels of management to believe they had a more mature program than they really have, and keep their expectations of their subordinates unrealistically high. The issue here is that management cannot fix what it does not know, so personnel need to be better at communicating what drives their stress.





Business Impact Summary

The data indicates that alerting systems are not operating in a generally efficient manner. 46% of incidents are automatically classified as critical alerts. Upon inspection, between 1% and 5% of tickets should be in this categorization. By itself this problem is unacceptable, but added to the fact that over 30% of incident alerts are false positives that should not have been generated in the first place, it is becoming easier to see why security teams feel stressed and overwhelmed. Research found that on average, analysts were spending 24 and 30 minutes to investigate each incident they received.

Given this amount of time and the volume of false alerts that are generated, teams are falling behind on alerts–creating an unworked backlog of 64% of tickets. This means analysts waste over half of their day looking for problems that are either insignificant or not really problems at all. They fall behind more each day, which is why dwell time for breaches is over six months. Many turn to “tuning” systems to reduce generated alerts, leading to the scenario where real alerts are never generated due to improper tuning.

While larger teams could solve the problem, trained personnel are not available and this particular solution does not scale. It also does not address the root of the problem. Ultimately, this is a tools issue. The systems are not given enough context at alert creation to properly classify the incoming alerts.

To succeed, tools must be made smarter by providing more useful context around the technical, financial, and behavioral aspects of the incidents. This will reduce the number of false positives and misclassified alerts so that only the real, most critical threats are at the top of the investigation pile. As the number of critical alerts will shrink, and improved upfront context shrinks the amount of time analysts spend per incident, a day in the life of a security pro will become significantly less stressful.

46% Percent of Tickets the System Prioritized as Critical

31% Percent of Tickets Identified as False Positives (Wasted Time)

64% Percent of Tickets NOT worked per day

52% Percent of Tickets Mis-prioritized by System (Wasted Time)

About Bay Dynamics

Bay Dynamics® enables enterprises to continuously quantify the financial impact of cyber risk based on actual conditions detected in their environment. The company's flagship product, Risk Fabric®, is a software platform that calculates the value at risk associated with specific threats and vulnerabilities, that when mitigated, measurably reduce cyber risk exposure. Using Risk Fabric, stakeholders across the business can prioritize their remediation activities and direct their limited resources at the risks that matter most. Risk Fabric benefits enterprises with a financial measurement of cyber risk that's based on current detectable conditions in the enterprise environment, gathered from existing security tools and business context. The platform also provides value-based prioritization of remediation, reduced regulatory risk, reduced costs, and improved timeliness of action by automating the delivery of personalized and prioritized vulnerabilities to line of business application owners responsible for remediation. For more information visit www.baydynamics.com.

Follow Bay Dynamics on Twitter at www.twitter.com/BAYDYNAMICS, on LinkedIn at www.linkedin.com/company/bay-dynamics/, and on Facebook at www.facebook.com/bay.dynamics.

Bay Dynamics and Risk Fabric are registered trademarks of Bay Dynamics, Inc. Other trademarks mentioned are the property of their respective owners.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com
3550.041817