

A photograph of a modern office building at night, with multiple floors visible through large glass windows. The interior lights are on, showing office desks, chairs, and some plants. The building is partially obscured by a dark, semi-transparent overlay on the right side of the image, which contains the report title and other text.

2019 Insider Threat Program Maturity Model Report

Survey and Analysis conducted by
Techvangelism & Insider Threat Defense

Sponsored by

Veriato

Table of Contents

Insider Threat Program Maturity Model Report

About This Report	3
About The Contributors	4
Key Findings	5
Insider Threat Program Maturity Model Report	
Preparing For The Threat	7
A Detailed Look At The 5 Levels	8
Benchinmarking Program Maturity	12
Program Maturity By Demographic	13
Program Support	14
Program Support Impact on Program Maturity	15
Budget	16
Budget Impact on Maturity Level	17
The Presence of a Formalized ITP Team	18
The Impact of Privacy	19
Communications	20
Tools In Use	21
Key Action Items	22
Key Considerations for Establishing an ITP Program	23

About this Report

The Insider Threat Program Maturity Model report was created to help security professionals assess their organization's ability to monitor for, detect, and respond to insider threats. By using a maturity model for reference, organizations can see where their program needs improvement, working towards an Optimized level of maturity. This maturity level allows the organization to dynamically align the program with current operations, responding quickly, efficiently, and effectively to both leading and active indicators of insider threat.

To provide context around the current state of Insider Threat Programs (ITPs), we surveyed 150 information security professionals to see at what level their program is in and what's influencing it. We've included this data in the report to provide you with insight into the necessary steps to mature your current program.

About the Contributors



Jim Henderson

Jim Henderson has over 15 years of hands-on experience in the development, implementation and management of complex enterprise Cyber Security-Information Systems Security Programs, Information Assurance Risk Management Programs and Insider Threat Programs for the U.S. Government, the Department of Defense, National Level Intelligence / Agencies Centers, State Governments, and large and small businesses.

Mr. Henderson has used his experience to develop and teach the highly sought-after Insider Threat Program Development-Management Training Course, and also provides Insider Threat Risk Management Services.



Nick Cavallancia

Nick Cavallancia is a cyber-security expert with over 25 years of enterprise IT and security experience. He regularly blogs, writes, and speaks on a wide range of cyber security issues, helping organizations, IT professionals, Managed Service Providers, and technology vendors understand the state of both insider and external threats, and how to build and execute a strategy to minimize risk.



Veriato

Veriato develops AI driven Insider Threat Security Solutions that provide companies with visibility into, and an understanding of the human behaviors and activities occurring within their network.

Thousands of companies in over 100 countries use their software. They provide world-class software that enables their customers to protect their most valuable assets, reduce risk, and gain unparalleled visibility into operations.

Key Findings

The 2019 Insider Threat Program Maturity Model report provides insight into how organizations today are addressing the threat of insiders. By looking at how factors like program support, budget, the presence of a formal team, and privacy impact program maturity, this report can provide a better understanding of what conditions are necessary to achieve the most effective program possible.



Mid-market organizations have the greatest amount of work to do. With a majority of these organizations given little to no budget and the most basic of C-level support, most insider threat programs are reactive in nature, allowing threats to occur before IT teams even respond.



The majority of organizations today have no formal team in place to establish policy and process, and to mature the program in response to both perceived and experienced threats.



Organizational concerns over privacy are minimal until an organization establishes a formal Insider Threat program and begins to proactively monitor for insider threats. From that point on, concerns over privacy diminish as program maturity increases.




Budget generally increases with program maturity. We saw the majority of budget amounts mirror the average program maturity trends, with increased amounts dedicated to the program to the highest levels of program maturity.



While most organizations enjoy overall support for an Insider Threat Program, members of the Finance team were the greatest blockers.



Organizations rely on log data, user activity monitoring, and eDiscovery (email) solutions consistently throughout every part of the model. A heavier reliance on video surveillance exists with less mature organizations, and the use of phone record details increased with program maturity.



Insider Threat Program Maturity Model Report

Preparing for the Threat

Insider Threat Program Maturity Model

Preparing for the Threat

The Insider Threat Program Maturity Model provides organizations with a way to benchmark their current ability to monitor, detect, mitigate, and respond to insider threats. The Maturity Model also helps to determine a path to further mature the existing program towards a metrics-centric, optimized program.



Insider Threat Program Maturity Model

A Detailed Look at the 5 Levels

The following pages provide specifics to both help identify your organization's current level of program maturity, as well as to better understand the difference in how more mature levels operate.

	 NONEXISTENT	 REACTIVE	 PROACTIVE	 PREDICTIVE	 OPTIMIZED
GOALS & OBJECTIVES	None	Respond to issues as they arise. Investigate as needed to identify what actions took place (if possible).	Monitor users with the highest risk to the organization for inappropriate activity.	Establish appropriate levels of monitoring to all employees. Identify potential threats early. Respond appropriately to both leading and active indicators of threat activity.	Ensure the insider threat program meets the changing needs of the organization through review, adaptation, and optimization of processes, monitoring, and responses.
AWARENESS	The organization has zero visibility into employee activity, nor into whether they have been or are a victim of an insider threat.	The organization is generally aware of insider threats but are notified by employees or third-parties that an act has taken place.	The organization is aware of insider threats and is taking steps to monitor activity in an effort to detect malicious threats by users deemed high-risk to the organization.	The organization is highly aware of insider threats. While the focus is on malicious insiders, the organization is focused on identifying leading indicators of threats in an effort to stop threats before the occur.	The organization has a mature view of insider threat risk - seeing it as something that moves throughout the organization, with every employee as a potential threat. Every source of activity detail is used to provide a full picture of employee risk.

CONTINUED ON NEXT PAGE >

Insider Threat Program Maturity Model

A Detailed Look at the 5 Levels

	 NONEXISTENT	 REACTIVE	 PROACTIVE	 PREDICTIVE	 OPTIMIZED
GOVERNANCE	None	None	Minimally established governance. Informal interaction between IT, HR, and Executive teams.	Oversight is established with a formalized team from IT, HR, Exec, Legal, and Security. Threat definitions exist. Basic process and policies are in place.	ITP Team includes key employees and a designated Senior ITP Official to head the team. Written policies and processes exist. The ITP team meets using a regular cadence.
RISK ASSESSMENT	None	None	Identified high-risk individuals and roles requiring monitoring.	Risk levels are defined, High- and Low-Risk roles are assigned. Specific one-off risk assessments occur for individuals.	Risk reviews, reassignment of risk levels and associated monitoring actions occur regularly for both roles and individuals.
POLICIES	None	None	Either none, or basic policies exist for high-risk individuals, driven by HR or IT.	Policies exist around BYOD, proper use of company resources, and maintaining confidentiality.	Policies are routinely examined to ensure they align with other changes in the program.

CONTINUED ON NEXT PAGE >

Insider Threat Program Maturity Model

A Detailed Look at the 5 Levels

	 NONEXISTENT	 REACTIVE	 PROACTIVE	 PREDICTIVE	 OPTIMIZED
MONITORING	None	None	Activity is monitored for pre-defined activity thresholds the organization equates as indicators of risk.	Activity is monitored for both leading and active indicators of threats based on both static definitions and behavioral analysis.	Activity is monitored for both leading and active indicators of threats based on both static definitions and behavioral analysis.
PROCESSES	None	None	Only informal processes exist around the review of activity and necessary response.	All employees are monitored for leading threat indicators using User Behavior Analytics (UBA) and User Activity Monitoring (UAM). Clear and defined processes are in place for high-risk scenarios.	All employees are monitored for leading threat indicators utilizing User Behavior Analytics (UBA) and User Activity Monitoring (UAM). Detailed processes are in place for specific low and high-risk scenarios, and are routinely evaluated and tested.

CONTINUED ON NEXT PAGE >

Insider Threat Program Maturity Model

A Detailed Look at the 5 Levels

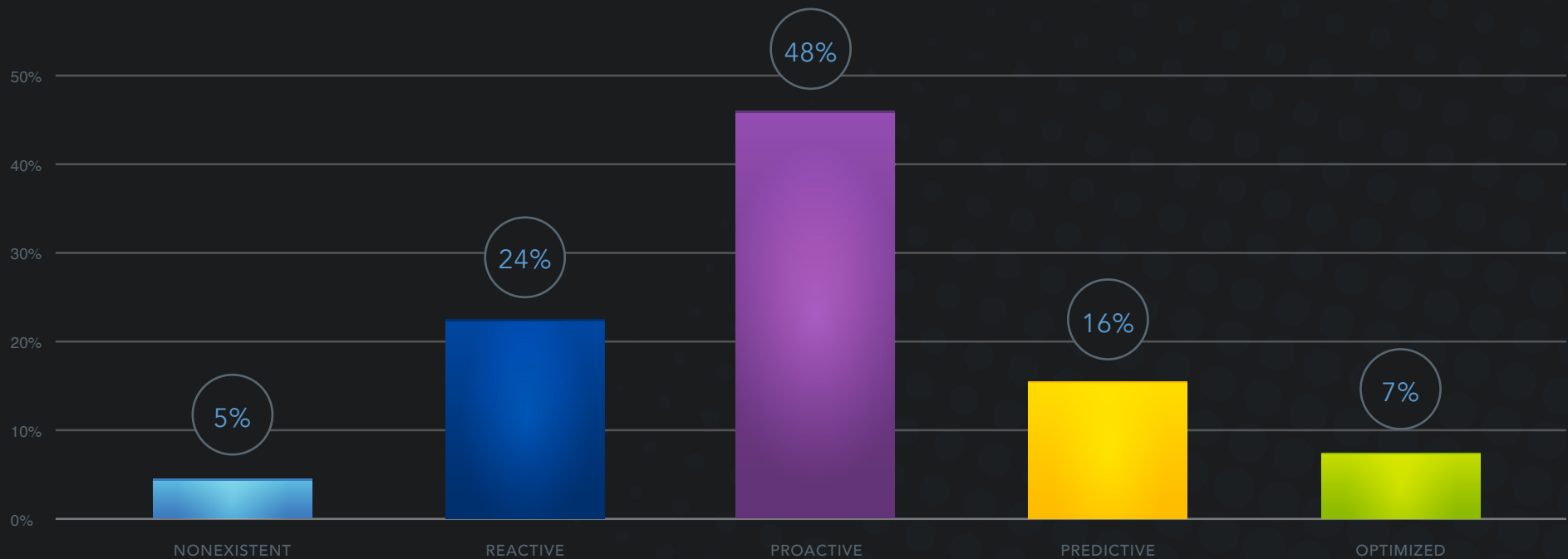
	 NONEXISTENT	 REACTIVE	 PROACTIVE	 PREDICTIVE	 OPTIMIZED
INTELLIGENCE SOURCES	None	None	Identified high-risk individuals and roles requiring monitoring.	Risk levels are defined, High- and Low-Risk roles are assigned. Specific one-off risk assessments occur for individuals.	Risk reviews, reassignment of risk levels and associated monitoring actions occur regularly for both roles and individuals.
COMMUNICATIONS & TRAINING	None	None	Basic Acceptable Use Policy in place.	Acceptable Use Policy, CIPA in used for all new hires.	Acceptable Use Policy, CIPA, & Security Acknowledgement are all signed by employees. Logon banners reaffirm proper usage, confidentiality, and security.

CONTINUED ON NEXT PAGE >

Insider Threat Program Maturity Model

Benchmarking Program Maturity

The majority of organizations rate themselves as being proactive in their approach to insider threats, putting their focus on the behavior of users identified as having the highest perceived risk to the organization. Activity is monitored using a variety of tools, with only informal processes in place around response.

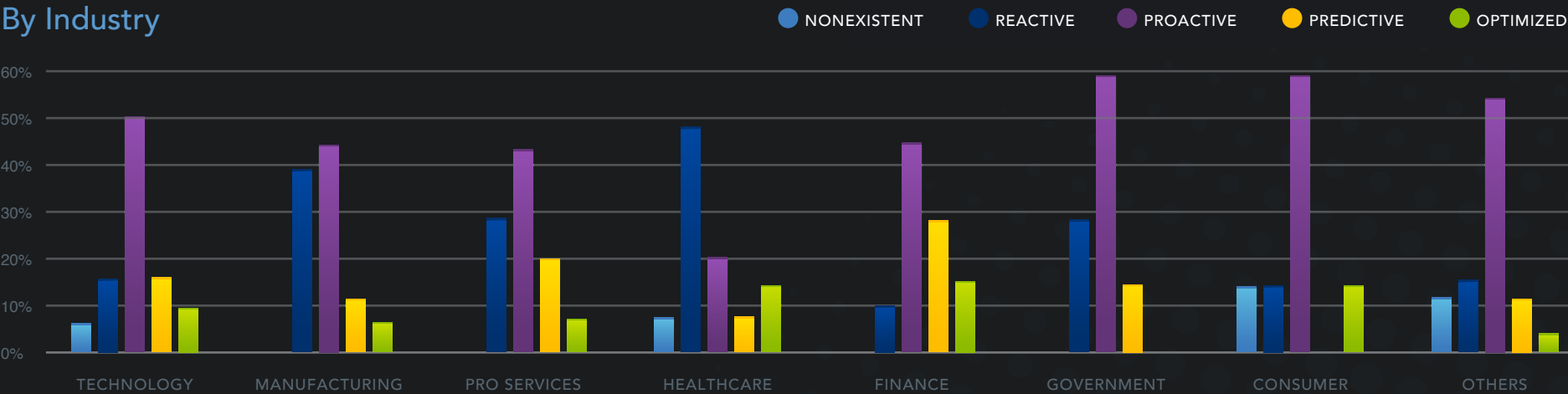


Insider Threat Program Maturity Model

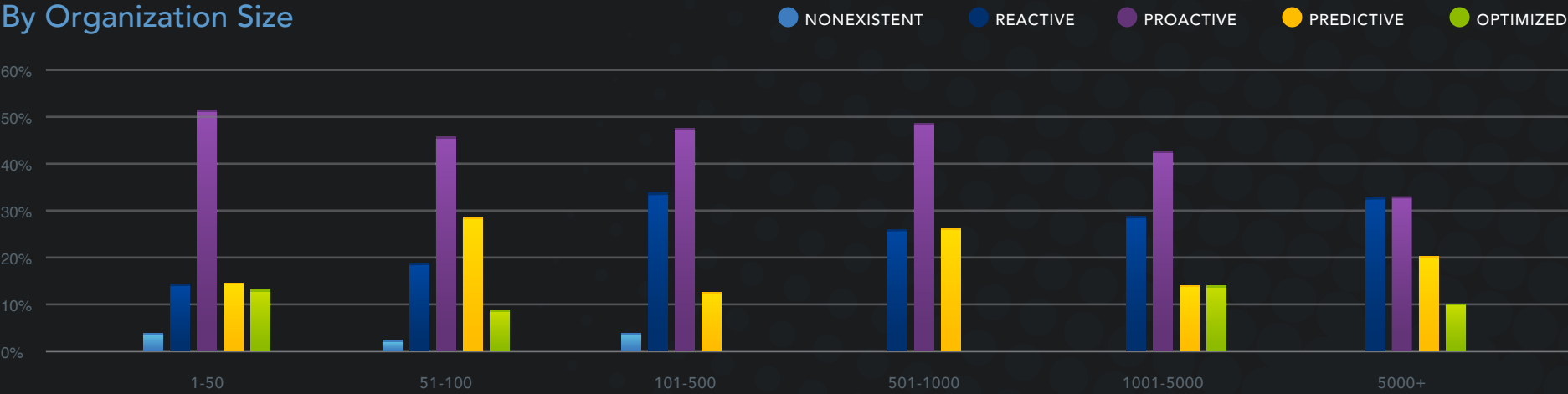
Program Maturity by Demographic

Breaking down program maturity by industry and organization size, you can further benchmark the program maturity of organizations similar to yours. From the results below, we see that the maturity levels are very low across the board. Even in the largest organizations where we would expect to see the most sophisticated security, less than 30% have either Predictive or Optimized programs in place.

By Industry



By Organization Size

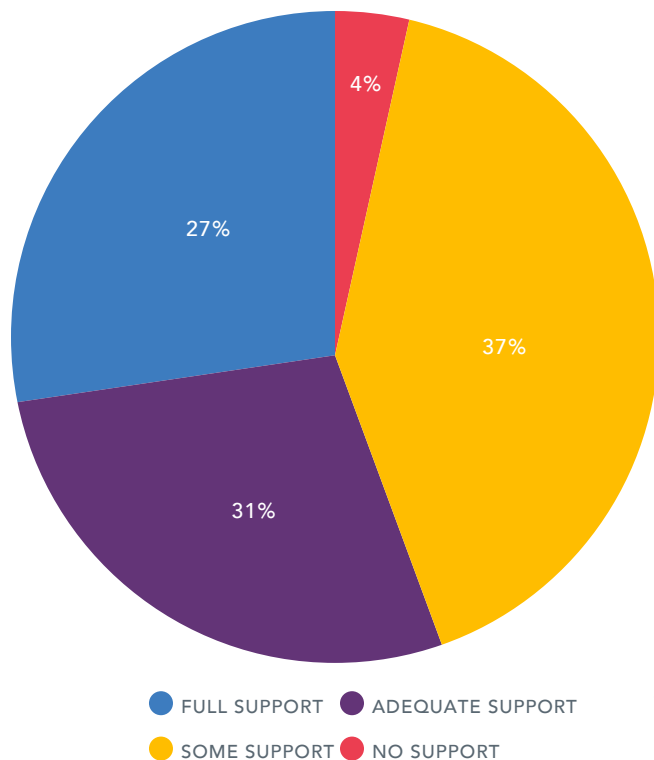


Insider Threat Program Maturity Model

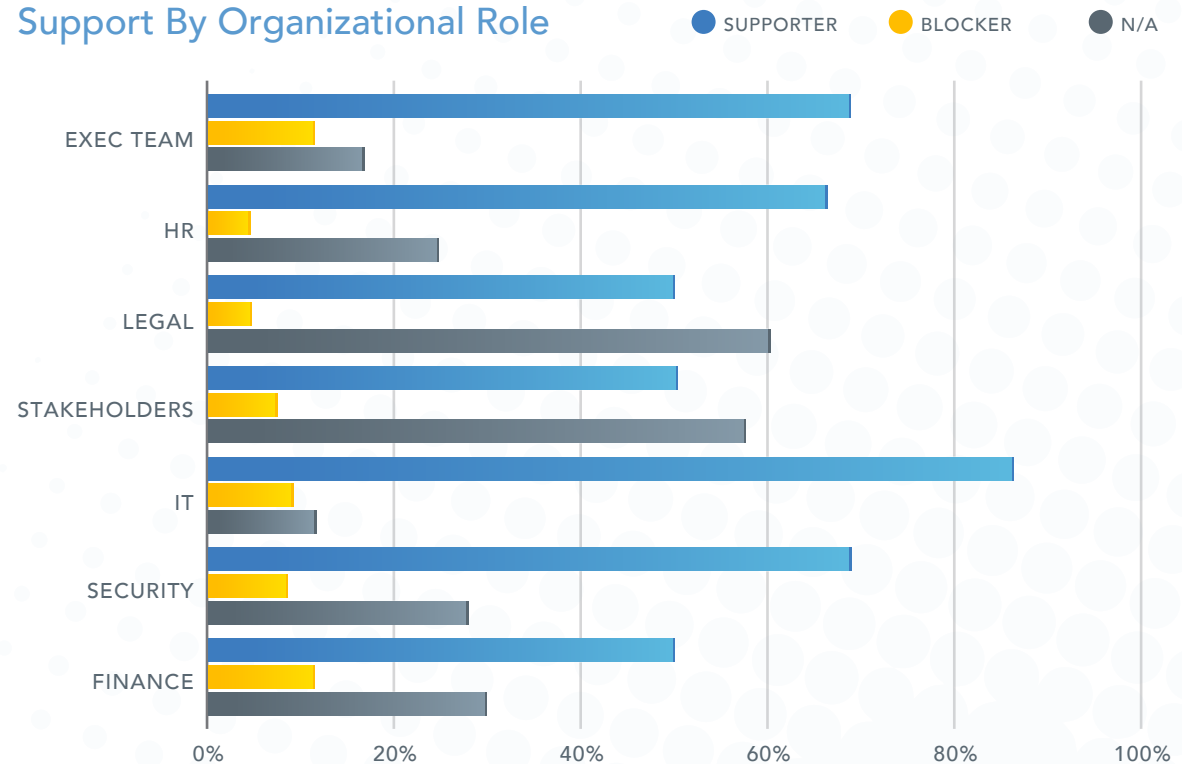
Program Support

The majority of organizations have some level of support for an Insider Threat Program. The largest instances of full support were found in smaller businesses (less than 100 employees), and the largest enterprises (5000+), with the largest instances of no support found in the mid-market (100-500 employees). The Finance, Consumer, Government, and Healthcare industries showed the most support for a program.

Nearly every role involved in an Insider Threat Program showed support for the program. Finance topped the list of those blocking the program. Communicating the value of the program – and the resulting cost savings to the organization through avoiding fraud or data breaches – is key to obtaining their support.



Support By Organizational Role

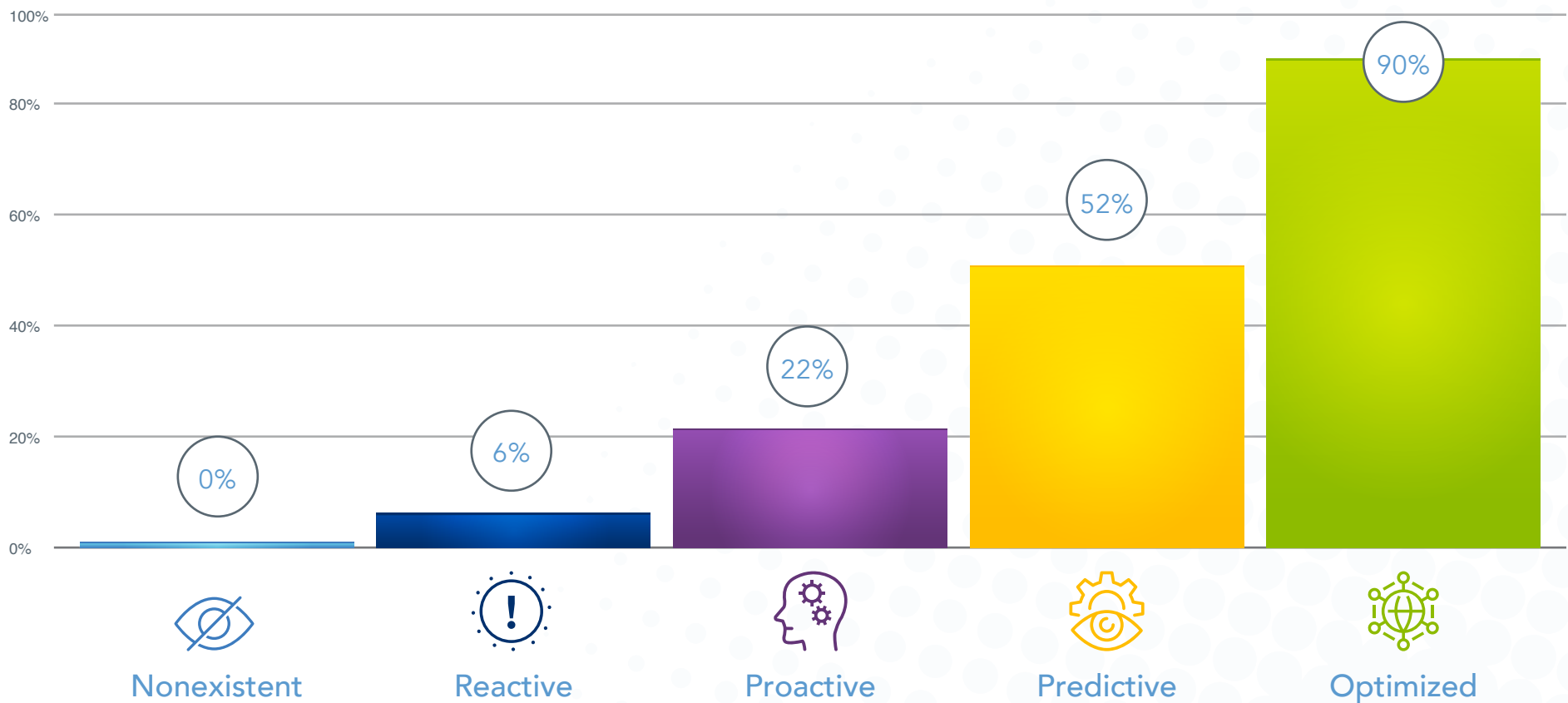


Insider Threat Program Maturity Model

Program Support Impact on Program Maturity

The maturity of an ITP can be greatly impacted by the degree of support from the organization. As shown below, there is a direct correlation between those organizations with program support and the maturity of that program.

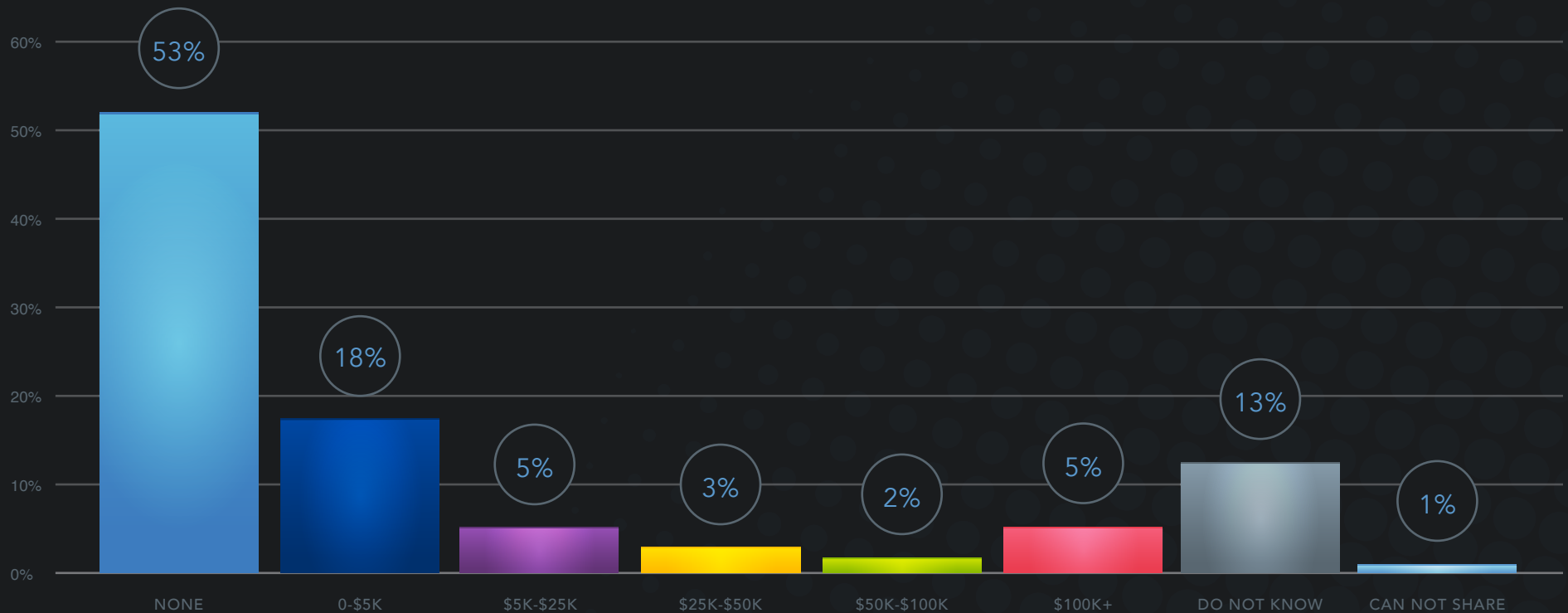
Percentage of organizations with full support for an Insider Threat Program



Insider Threat Program Maturity Model

Budget

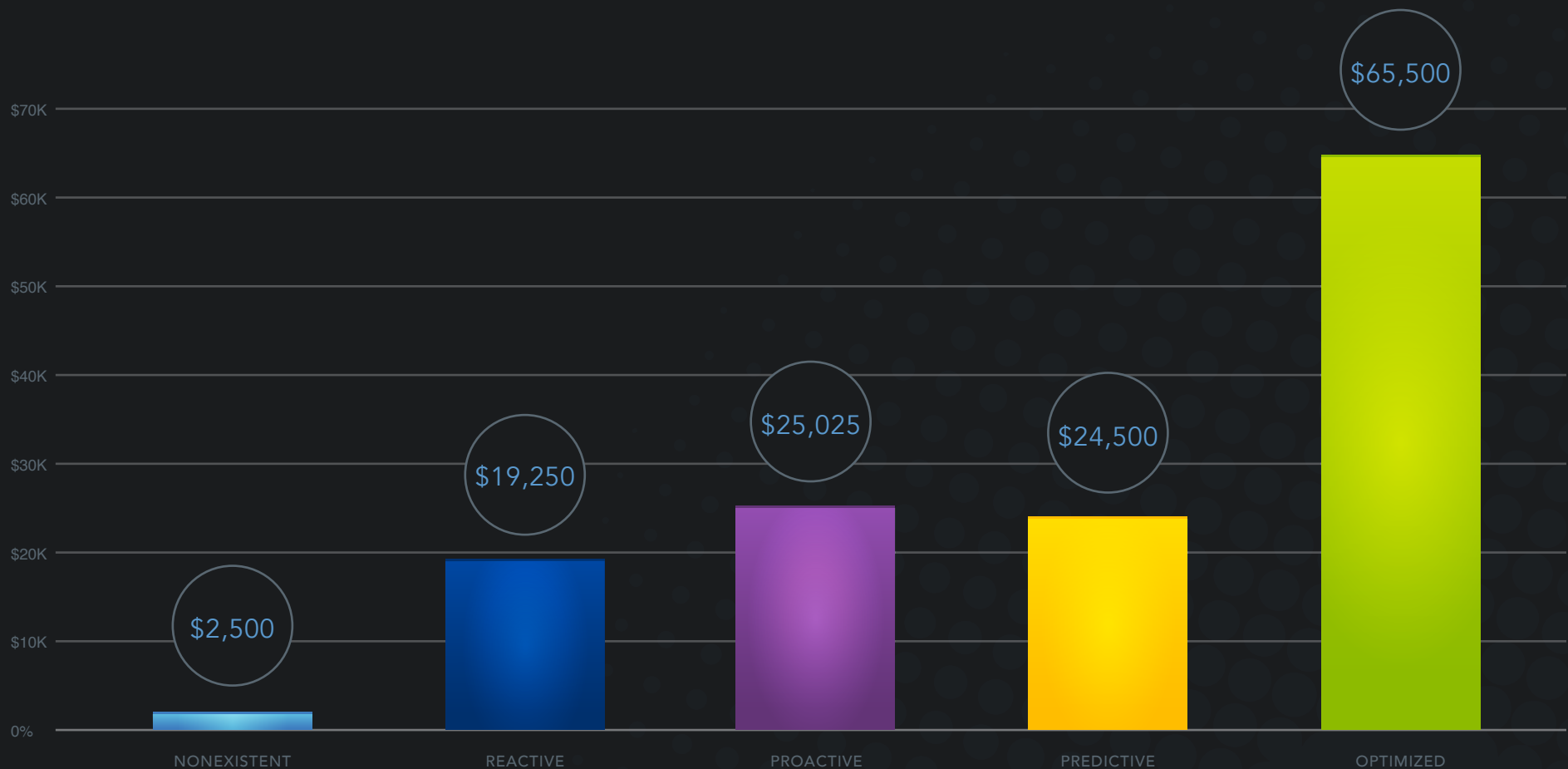
The average budget was around \$27,500 per year. A large percentage of organizations allocated no budget for an Insider Threat Program despite the vast majority supporting the idea. Of those organizations citing no budget, 92% were small or medium businesses (less than 500 employees), with the remaining 8% spread across all organizational sizes.



Insider Threat Program Maturity Model

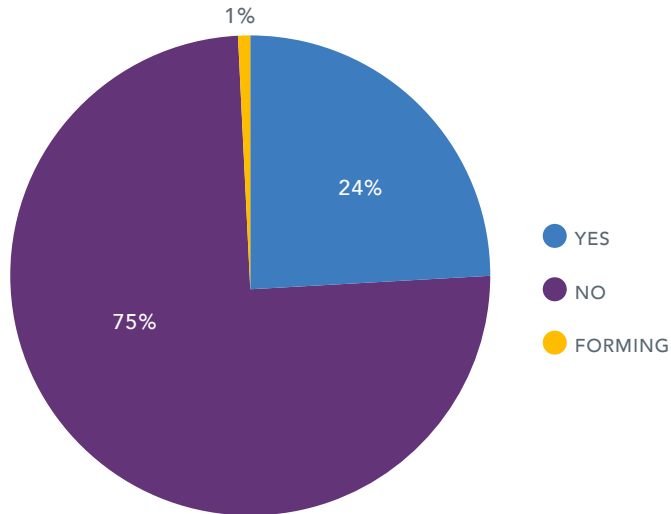
Budget Impact on Maturity Level

Not surprisingly, as program maturity increases, so does the amount of budget allocated. The chart below shows the average budget allocation for each level of maturity. Those with a nonexistent program spend very little or nothing at all towards addressing Insider Threats, while Reactive, Proactive, and Predictive allocate similar budget amounts to address the problem. It's not until organizations get to an Optimized maturity level that we see a material increase in the average budget.



Insider Threat Program Maturity Model

The Presence of a Formalized ITP Team



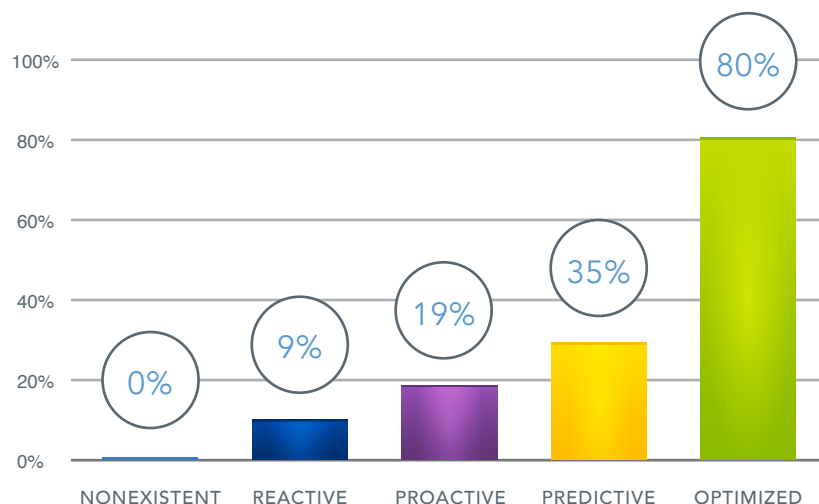
One of the signs of a mature Insider Threat Program is the establishing of a formal program team. This team can be made up of representatives from every supporting department within the organization. It should focus on identifying where risk exists within the organization, what types of monitoring are appropriate to detect inappropriate behavior, as well as establish and review policies and processes that will be used when indicators of an insider threat are realized.

Three-quarters of programs have no formal team, which puts the effectiveness of those programs in question.

Of the nearly one-quarter that do have a formalized ITP team, two-thirds of them have a designated Senior Official who heads up the team.

A majority (80%) of Optimized programs have a formal team, with that percentage dropping significantly to 35% of Predictive programs, 19% of Proactive, and 9% of Reactive programs. Those organizations with a nonexistent program obviously have no formal team in place.

Presence of senior official by program maturity



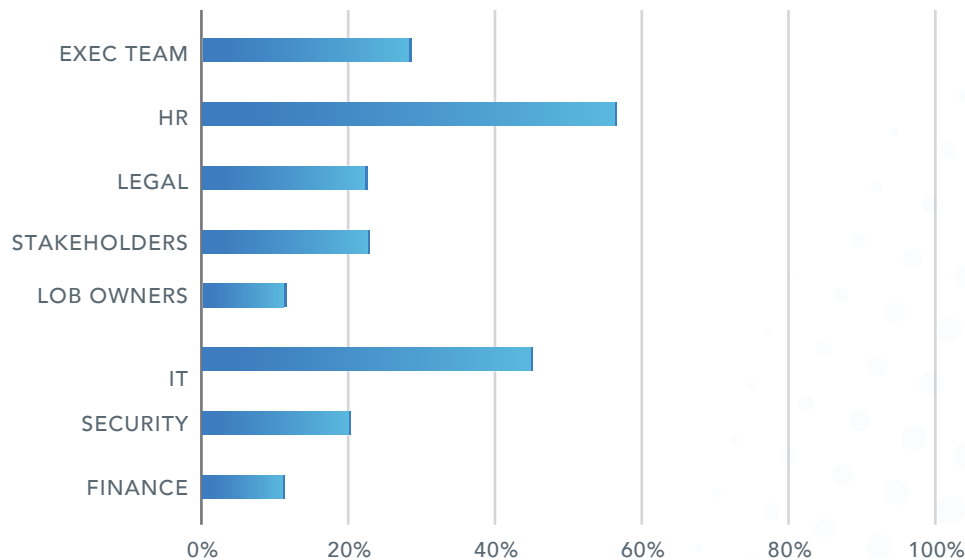
Insider Threat Program Maturity Model

The Impact of Privacy

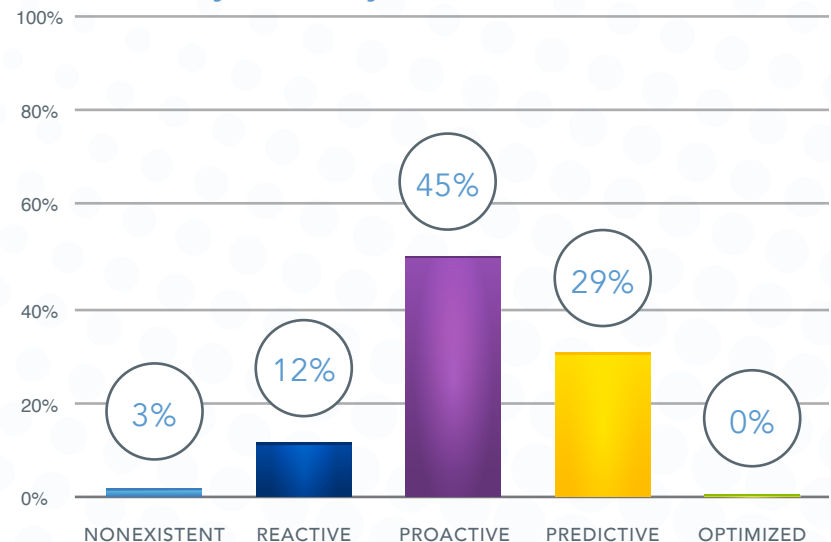
Employee privacy can be a concern for organizations looking to implement an Insider Threat Program. Surprisingly, only 23% of organizations showed privacy concerns. Of those, Human Resources ranked as the role most commonly demonstrating privacy concerns.

Privacy becomes a material issue when organizations reach a Proactive level of program maturity. As organizations mature beyond Proactive and the Insider Threat Program moves towards Optimized, the concern for privacy drops, with 0% of organizations at an Optimized level being concerned about privacy.

Percentage of Orgs Concerned About Privacy By Role



Breakdown of Organizations with Privacy Concerns by Maturity Level

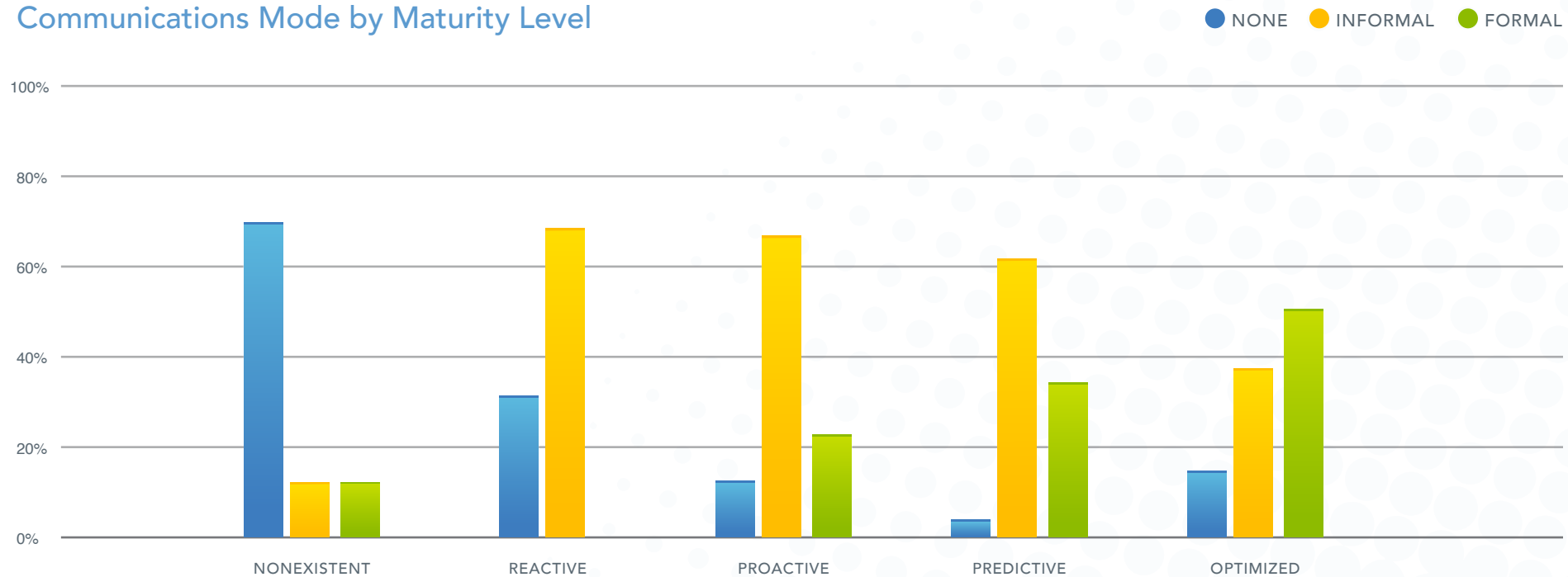


Insider Threat Program Maturity Model

Communications

Most organizations utilize informal communications between members, only communicating when an insider issue arises using no formal process. The 21% of organizations using formal modes of communication have established processes that are followed to facilitate appropriate response to potential and active insider threats. When breaking down communications by maturity level, Reactive is expectedly informal. Proactive programs are split almost evenly between the two modes of communication, acting as the tipping point. Once organizations reach both Predictive and Optimized, the majority of communications are formal.

Communications Mode by Maturity Level

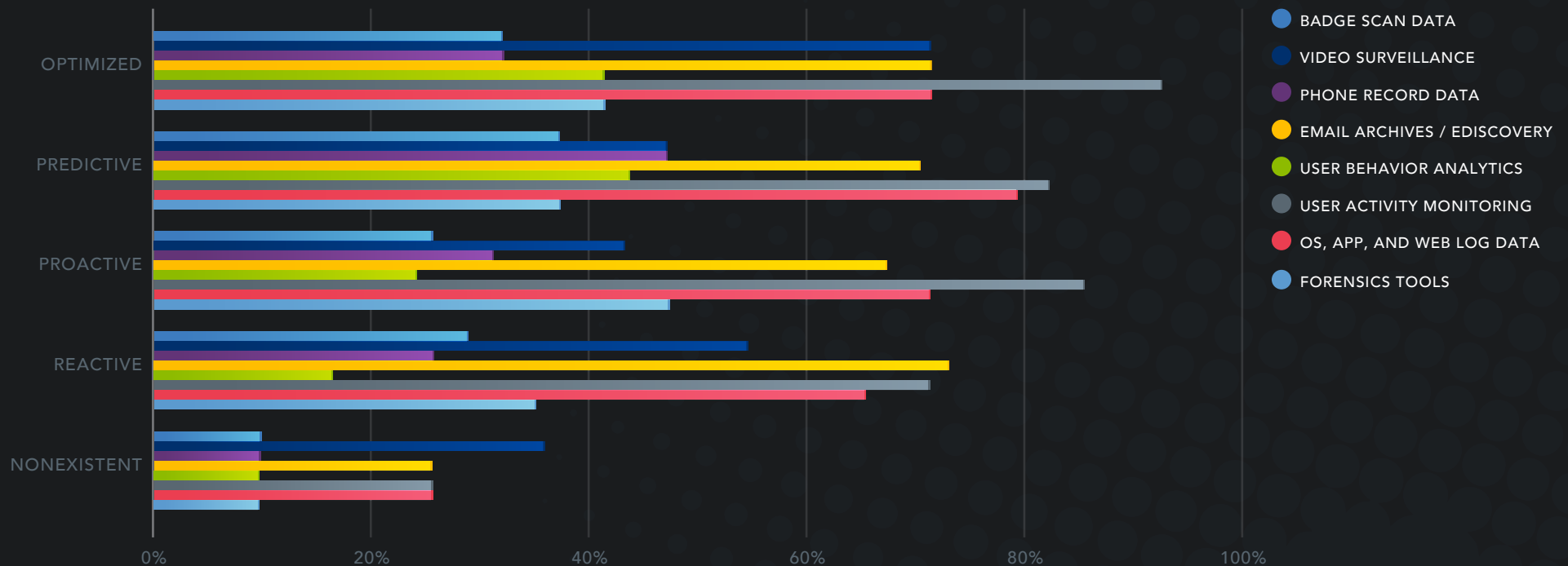


Insider Threat Program Maturity Model

Tools In Use

In general, organizations are relying heavily on log data, user activity monitoring, and email-based eDiscovery. We saw a growth trend in nearly every tool category as the maturity levels grow from Nonexistent to Optimized, with more mature programs showing an increased emphasis on user activity monitoring, forensic tools and user behavior analytics. Badge scan and phone record data seems to be of secondary concern for most organizations, with video, email, user activity, and log data as primary monitoring sources.

Tools in Use to Address Insider Threats



Key Action Items

Support

Solicit the support of the C-Suite and key departments to ensure funding can be secured, tools can be put in place, teams can be formed, processes can be crafted, and policies can be enforced. Discuss the program in terms of the individual stakeholder, telling them how their concerns are addressed and covering how it directly benefits their part of the organization.

Team

Putting an Insider Threat Program team together helps to align the interests of all its members – IT, HR, Legal, Security, and the C-Suite. Assign a Senior Office to lead the team and focus your efforts on establishing where risk exists in the organization, how to monitor for it, and formalize a response when discovered.

Communications

Formalized communications are a product of a formal team in place. Establish processes – and the communications necessary to facilitate them – to ensure the right individuals or departments are made aware of activity and can respond in a timely manner, reducing risk.

Budget/Tech

The budget for an organization's Insider Threat Program will be dependent on its size and needs. But, with the average program budget of a little over \$27,500, it's evident that the more successful programs do have some monies dedicated to the effort. Much of the budget goes to tools, so the solutions you choose should provide you with visibility into user behavior – as, it's behavior that determines whether an action is malicious or beneficial to the organization.

Key Considerations for Establishing an ITP Program

Obtain executive buy-in. This will give the leverage to work across organizations, secure budgeting and establish the foundation of the ITP Program.

Consult with legal counsel early and frequently to ensure the ITP Program can be leveraged appropriately, consequences are defined and that policies are enforceable and in line with organizational culture and privacy concerns.

Define the process for how to respond to an insider threat situation including who is notified, who will own components of any investigation and remediation. This may include IT, Security, HR and executive personnel.

Create an inventory of critical data to define the focus of the ITP Program.

View internal threats holistically as you would external threats. Include not just employees but also contractors and vendors with access to the network.

Identify existing technologies which may augment the ITP Program such as systems used by HR and IT.

Establish clear acceptable use policies for how employees are allowed to use corporate resources such as workstations, mobile devices and networks. Ensure policies regarding BYOD devices are specified.

Identify resources to assist HR in employee screening to maximize insider threat prevention before onboarding.

Invest in the correct tools to identify, prevent and mitigate insider threats. A mature ITP program will include technologies that give visibility into the endpoints, the network, user access and critical data of the organization.

Include ITP Program communication as part of the onboarding and annual training processes. This will generate awareness and set expectations.