ESG Brief

The ESG Cybersecurity Maturity Model

Date: October 2014 **Author:** Jon Oltsik, Senior Principal Analyst

Abstract: *As part of its research, ESG regularly uses a scoring system to divide survey populations into three distinct segments in terms of their cybersecurity skills, resources, and technologies: advanced organizations, progressing organizations, and basic organizations. The differences between these groups are extremely prescient as they illustrate consistent weaknesses, progressions, and ultimately best practices. This ESG brief looks at the three segments in four areas: their cybersecurity philosophies, people, processes, and technologies. This comparison represents a cybersecurity maturity model. CISOs can use this model as a guideline to assess their current status, plot out next steps, and avoid some of the pitfalls experienced by others.*

Overview

ESG publishes several research reports each year based upon in-depth surveys of security professionals working at enterprise organizations (i.e., more than 1,000 employees). Earlier this year, ESG published a report on network security, *Network Security Trends in the Era of Cloud and Mobile Computing*, based upon a survey of 397 enterprise security professionals. In 2013, ESG also published a report, *Advanced Malware Detection and Protection Trends*, based upon a survey of 315 enterprise security professionals.

As part of its security research projects, ESG regularly develops a scoring model in order to divide the entire survey populations into three segments based upon their infosec resources, strategies, and skill sets: advanced organizations, progressing organizations, and basic organizations. Based upon years of experience with this methodology, the ESG research segmentation models tend to follow a consistent pattern. Approximately 20% of enterprise organizations can be considered "advanced," about 60% fall into the "progressing" category, and the remaining 20% can be classified as "basic" with regard to information security.

The ESG Cybersecurity Maturity Model

While advanced, progressing, and basic organizations come in all sizes and industries, they tend to exhibit similarities with regard to their information security philosophies as well as their people, processes, and technology behavior. These patterns are represented as a maturity model within this ESG brief (see Table 1).

Table 1. The ESG Cybersecurity Maturity Model

Category	Basic Organizations	Progressing Organizations	Advanced Organizations
Philosophy	Cybersecurity is a "necessary evil."	Cybersecurity must be more integrated into the business	Cybersecurity is part of the culture.
People	CISO reports to IT. Small security team with minimal skills. High burnout rate and turnover.	CISO reports to COO or other non-IT manager. Larger security team with some autonomy from IT. Remain overworked, understaffed, and under-skilled.	CISO reports to CEO and is active with the board. CISO considered a business executive. Large, well-organized staff with good work environment. Skills and staff problems persist due to the global cybersecurity skills shortage.
Process	Informal and ad-hoc. Subservient to IT.	Better coordination with IT but processes remain informal, manual, and dependent upon individual contributors.	Documented and formal with an eye toward more scale and automation.
Technology	Elementary security technologies with simple configurations. De-centralized security organization with limited coordination across functions. Focus on prevention and regulatory compliance.	More advanced use of security technologies and adoption of new tools for incident detection and security analytics.	Building an enterprise security technology architecture. Focus on incident prevention, detection, and response. Adding elements of identity management and data security to deal with cloud and mobile computing security.

Source: Enterprise Strategy Group, 2014.

Profile of Basic Organizations

As previously mentioned, about 20% of organizations fall into the "basic" category. These firms can be described as follows:

- **Philosophy: Information security is a "necessary evil."** Basic organizations have a history of dismissing "good security" and adopting "good enough security." In other words, they tend to cut corners in terms of security investment as much as possible, opting for only what's absolutely necessary. These decisions reflect the fact that basic organizations really don't understand the relationship between IT-based business processes and strong security, thus they face a higher level of IT risk than they understand. In many cases, the information security focus at basic organizations tends to skew toward elementary threat prevention and meeting regulatory compliance requirements rather than protecting IT assets, valuable data, and employees or detecting/responding to actual security attacks.
- **People: Security administrators and compliance wonks.** Cybersecurity is considered an IT sub-discipline at basic organizations. As such, they tend to have technology-focused CISOs who report to the CIO or another IT manager (if they have a CISO at all). The security group tends to be lean, with many standard security tasks handled by the IT staff. Since basic organizations consider security a low priority, they can't recruit top talent, and those security professionals they do hire tend to be overworked and frustrated. Not surprisingly, basic organizations experience high turnover within the security staff.
- **Processes: Tend to be informal and manual.** Since the security team is understaffed and under-skilled, they tend to spend a lot of time dealing with the emergency Du Jour. This leaves little room for planning, skills development, or creating an appropriate security strategy. Security processes tend to be ad hoc as security

professionals have limited ability to influence the IT staff at large. All security activities depend upon individual skills and techniques rather than formal processes. This creates a visible security gap when key personnel leave the organization.

- **Technology: No-frills point tools in logical areas.** Basic organizations implement pedestrian security technologies like firewalls, endpoint antivirus software, IDS/IPS, and perhaps log management tools. Advanced security features are eschewed for fear that they might impact performance or disrupt the business. Each tool is implemented and managed on its own with little to no interoperability across technology silos. Security monitoring is done on a sporadic basis and is skewed toward compliance reporting and auditing rather than situational awareness. This leaves basic organizations with visibility gaps between scans and no way to assess their overall security status across the entire organization.

Profile of Progressing Organizations

Over the last few years, the 60% of organizations making up the "progressing" segment have likely had some type of cybersecurity awakening. It's not unlikely that these firms experienced a security breach or witnessed a breach at another similar organization in their industry. Whatever the motivation, progressing organizations are much more serious about cyber risk than the basic crowd. These distinctions are exhibited in the following ways:

- **Philosophy: We need to get more engaged around cybersecurity.** Progressing organizations recognize that cybersecurity issues can impact them at any time and cause an undue amount of harm. This leads to a number of proactive steps. First, cybersecurity risk issues reach a business level, although executive management and board members may not know much beyond the fact that they have to pay attention. Progressing companies are motivated to "do something" so they tend to proceed beyond incident prevention to incident detection by adding additional layers of security defenses and management tools. While this may lead to some security improvements, it can add overhead and additional operational complexity as well.
- **People: Establish a real cybersecurity group.** Progressing organizations will typically have a CISO or similarly titled individual leading the security effort and reporting to a COO, risk officer, or other non-IT manager. While this person typically has a technology background, business executives willingly work with the CISO to bridge the business/cybersecurity divide. The security team at progressing organizations tends to have good skills, and the ability to provide input and security oversight over the IT team. Nevertheless, there are communications issues where security is "out of the loop," especially with regard to new IT initiatives like cloud and mobile computing. While progressing organizations place an emphasis on infosec, they still find it difficult to recruit top talent, which translates into an IT security team that is over worked, understaffed, and lacking some critical skills.
- **Processes: Sort through confusion and finesse toward formal processes and automation.** In spite of their commitment and enthusiasm, progressing organizations often make the mistake of adding new security technologies with little compensatory effort to re-engineer security processes. It is not unusual for progressing companies to improve processes based upon the skills and size of the security organization, but incremental progress is often diluted as progressing organizations implement more sophisticated hands-on security tools. Ultimately, security operations complexity becomes an issue as progressing organizations realize that they aren't able to capitalize on all of their new security technology capabilities. This ultimately leads to focused grassroots projects to document, formalize, and automate security processes.
- **Technology: Implement advanced tools at all costs**. As previously mentioned, progressing companies move beyond the basics, get more engaged with the security capabilities of existing technologies, and dabble with newer tools. For example, progressing companies are more likely to enable real-time protection features in endpoint security software or build a hierarchical network architecture using VLANs, ACLs, and firewall rules. Progressing organizations also understand that security analytics should go beyond compliance reporting, so they are more likely to deploy SIEM, NBAD, or other types of tools. As part of the advancement from prevention to detection, progressing organizations are also likely to deploy some type of advanced malware gateway, albeit in passive mode only. Finally, progressing organizations often organize their personnel and security tools into some sort of SOC, although it may be nothing more than a common room for people and

monitors. Progressing companies deserve kudos for their technology efforts, but they frequently discover that they are in over their heads sooner than anticipated.

Profile of Advanced Organizations

The remaining 20% of organizations can be considered "advanced" as they possess the best cybersecurity skills, resources, and technologies. It is important to note, however, that advanced organizations are often the most attractive targets for cyber adversaries, so they develop strong security hygiene and best practices because they have to. Advanced organizations are characterized as follows:

- **Philosophy: Cybersecurity is part of the organizational culture.** Advanced organizations understand that security must be "baked-in" to business processes as they align more closely with IT. Consequently, business leaders and corporate boards are directly involved in IT risk assessment and cybersecurity strategy, while CISOs often report directly to the CEO and are treated as business executives rather than IT geeks. This may explain why CISOs at advanced organizations are passionate about making strong security a business enabler. Business leaders act as cybersecurity champions and all employees go through awareness training on a regular basis. While advanced organizations have the highest infosec budgets, they tend to remain diligent about the threat landscape and are willing to address new, unanticipated risks sooner rather than later. Finally, advanced organizations tend to manage cybersecurity with a series of metrics in order to gauge whether they are improving and if so, by how much.
- **People: The best and brightest—if we can find them**. Advanced organizations recruit and hire the best talent they can find, from the CISO to junior administrators. They also pride themselves on creating the right work environment for cybersecurity professionals. For example, many advanced organizations are willing to invest in continuous education programs and give their top cybersecurity staff members leeway to work with industry ISACs, present at security conferences, and interact with engineers working for security technology partners. In spite of these organizational efforts, advanced organizations are impacted by the acute global cybersecurity skills shortage and still have difficulty recruiting and retaining security professionals. This may explain why advanced organizations are also the most aggressive when it comes to working with professional and managed providers for security services. CISOs at advanced organizations are smart enough to know when they need professional services for a particularly esoteric security skill set and when they can outsource mundane security tasks.
- **Processes: Strive for military precision.** While progressing organizations realize that they need to do something about security complexity, advanced organizations are already streamlining all they can. For example, many advanced organizations are focused on various workflows to improve collaboration between security and business managers on one hand, and the security team and IT on the other. Advanced organizations also realize that even the best and brightest security teams can't possibly keep up with the scale and scope of cybersecurity threats. Consequently, they are leaning on advanced intelligence and technology integration to help them automate processes for risk management and incident detection/response. Finally, advanced organizations collect and analyze as much data as possible so they can adjust their tactics and prioritize their workloads effectively and efficiency. They also use data analysis to gauge their performance and make improvements when needed.
- **Technology: Identity, integration, and data security.** Like progressing organizations, advanced firms know they need new security technologies for defense-in-depth and security analytics. They too have SOCs, but they differ from progressing organizations in that they realize that additional point tools will solve old problems and create new ones simultaneously. To alleviate this conflict, advanced organizations are moving in a different direction by building an integrated security technology architecture that spans the enterprise. This type of architecture features central command-and-control, distributed enforcement, cloud-based threat intelligence, application-layer message exchange, and a massive data collection, processing, and analysis effort. Advanced organizations are also taking a leadership role in two other areas: identity and access management (IAM) and data security. On the IAM front, they are making identity a foundational component of security by using disparate identity attributes (i.e., user, role, device, network, location, time-of-day, etc.) to create and enforce granular access policies that can enable business processes while

managing IT risk. Advanced organizations are also doubling down on data security to discover, classify, lockdown, and monitor their most sensitive and valuable data. This emphasis on IAM and data security is especially important as internal IT gives way to the dynamic and distributed worlds of cloud and mobile computing.

The Bigger Truth

The ESG maturity model presented here should provide CISOs with some guidelines on where they are today, where they need to go, and the best ways to proceed while avoiding inevitable detours. As a final thought, ESG offers these recommendations for basic, progressing, and advanced organizations:

- **Basic organizations should seek immediate help.** Those basic organizations that "see the light" must realize that they are woefully behind and may be too far gone to dig themselves out of their cybersecurity holes alone. Rather than focus on infosec skills, basic organizations may be better served by working on their contract management and legal skills. Armed with these strengths, they should then seek out the best managed security service providers with industry knowledge and comprehensive coverage.
- **Progressing organizations need to think in terms of the big picture**. Progressing organizations often face a paradoxical situation where they are so busy that nothing gets done. Rather than lots of starts and stops on tactical initiatives, progressing organizations must take the counterintuitive step of slowing down. Start with an assessment, some penetration testing, and an effort to align cybersecurity with business and IT initiatives. This should help identify some obvious weaknesses but the security team must remember to connect all the dots between technologies along the way. Finally, CISOs at progressing organizations must concentrate on process automation for attaining operational efficiency or all other efforts will be marginal at best.
- **Advanced organizations need a three- to five-year plan.** In the 1990s, many enterprise organizations replaced departmental applications with integrated ERP systems. This effort was more difficult than many firms anticipated and was fraught with pitfalls, but those organizations that persevered were able to reap rich benefits in terms of business intelligence, agility, just-in-time supply chains, and automated business processes. ESG sees this situation as analogous to the current transition with enterprise security. CISOs need to recognize that cybersecurity technology integration won't be easy, but if done right, it will be well worth the effort. To proceed properly, large organizations should create a three- to five-year cybersecurity integration plan encompassing all aspects of their security technology. The plan should outline timeframes and project phases as well as define milestones and metrics to assess progress. Project objectives should adhere to what ESG calls the CISO triad: security efficacy, operational efficiency, and business enablement.