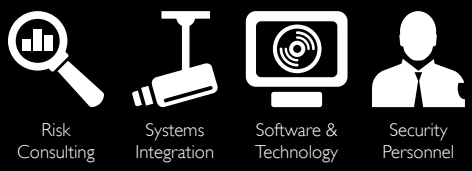
G4S Canada
Corporate Risk Services

Whitepaper



Maturing Your Security Program

Robert Hastings

In my experience, most organizations see security as a set of processes. That is, the security department (or function, if it is under another department) is a part of the organization that does things. These can include patrolling the building, checking doors, watching video surveillance monitors, and checking visitors in and out of the property. And that's what a security department is for: to do certain expected actions, and nothing more than that.

Imagine treating any other part of the organization in the same way. Finance, for example. Most organizations, whether public or private sector, have a financial function or department. And finance does things: takes in invoices, issues bills, makes payments, manages payroll, and so on. However, it would be very unusual, except in a very small or tightly-knit organization, to see finance's purpose as only performing these expected actions. Finance is expected to do much more: forecast quarterly results, manage cash flow, procure necessary equipment, predict the financial needs of the organization in the long-term, etc.

The reason that we expect more from finance than we do from security is twofold. First, most organizations are more worried about financial risk than security risk. Thus, security is allowed to just act and react, while finance also has to manage and predict. Second, security managers are used to acting and reacting, while financial managers are used to managing and predicting. Thus, there is some comfort in the status quo.

Unfortunately, neither of these reasons is very persuasive. At a certain level, security risk and financial risk converge. In a retail environment, for example, the risk of loss of merchandise -- a security risk -- produces a cost to the business -- which is a financial risk. Similarly, in a healthcare environment, the risk of loss of patient records -- a security risk -- produces a cost to the hospital or healthcare centre, through lawsuits if nothing else -- and this is a financial risk.

Similarly, while the status quo may be comfortable and familiar, no part of a complex organization can be permitted to just act and react. Whether it's finance, security, legal, human resources or sales, all parts of the organization need two key features: scalability and repeatability of their processes. Put simply, this means that whatever a part of the organization does, it has to be possible to do it again, possibly in a different location and with different personnel. And, whatever a part of the organization does, it has to keep doing it as well (if not better) as the overall organization grows and changes.

No one managing a business or other organization would accept that the finance department is no longer able to perform its function because one key person had moved on, or because the business was too big or had changed too much. The same applies to the security organization: everything that the security department does must be scalable and repeatable. And if the security department has these features, then it will also become a department that does more than just act and react.

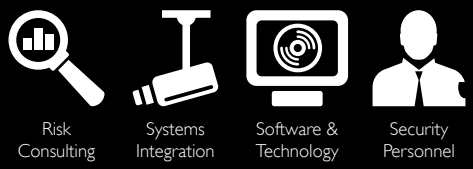
Maturity Models

Getting a security department from acting and reacting to being scalable and repeatable requires understanding the level of

For more information:
solutions@ca.g4s.com • www.g4s.ca • 1-888-717-4447

Maturing Your Security Department

Robert Hastings



maturity that the department has. This is not a concept that many security managers have been exposed to, in my experience, but it is important for justifying the role of security within the broader organization. (In fact, maturity models are used to justify the role of any department within a broader organization.)

It's well known that security is a cost centre, that generates no revenue and produces no profit. The value of a security department is in its ability to manage and mitigate security risk. All businesses and other organizations have a certain tolerance for risk. Risk can't be eliminated entirely, and controlling one source of risk may require accepting risk from another source. The core role of the security department, then, is to align its resources to manage security risk within the overall risk tolerance of the organization.

As organizations grow and change, this can become extremely challenging for a security manager. Whenever security managers experience these challenges, that means the security department needs to mature in order to continue to fulfill its function and produce value for the organization. Immature security departments -- or, to be very exact, security departments that are not mature enough for the organization -- increase the organization's exposure to risk. And as if that weren't bad enough, immature security organizations usually don't know that they have exposed the organization to increased risk.

If you have security cameras and card readers, they will continue to function even as the organization grows. And if you have security guards, they will continue to guard -- patrol, check doors, file reports, and so on. All that activity and equipment doesn't stop because the organization has undergone a change of some kind or an expansion. However, the needs of the organization may have changed, and so the practices of the security department may need to change as well. Maturity ensures that security needs and risks are identified, strategies are developed to mitigate them, and that security plans reach the level of front-line security guards.

Maturity models can be divided into five categories. And each level of maturity is appropriate for a certain kind of organization. Very small organizations will function very well with an immature (level 1) security department. By contrast, very large, global organizations, or organizations with a lot of internal operational complexity, require a security department that is at or close to perfect maturity (level 5). The point of maturity models is not to increase the complexity of providing security. The point is to make sure that the security department is as complex as it needs to be, in order to keep up with its core purpose of mitigating security risk. Most organizations that I have seen have a basically mature (level 2) security department. And sometimes that works -- and sometimes it doesn't.

Level 1: Immature.
An immature security department is unorganized and is not being managed in an active, ongoing way. Information (security metrics) is not being collected or analyzed. Security managers adopt a hands-off approach to providing security. Talent and individual effort of members of the security team is what leads to the success or failure of the program. Immaturity is often hard to detect, as the program will work as long as the level of risk is within the ability of the individual members to mitigate.

Level 2: Basic Maturity.
At this level, the security department has become somewhat organized. Processes exist, not just individuals taking actions, and these have some loose formal documentation. At this level, security processes can be repeated and exceptional individual effort is not required for success. It is still difficult to scale the security department if the organization grows or becomes more complex.

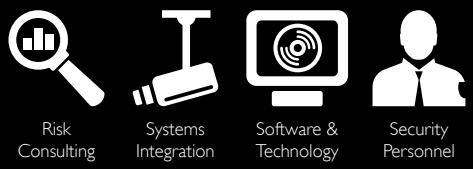
Level 3: Medium Maturity.
At this level, the security department is even more organized. Processes are documented more formally, and more processes are documented. Processes have been standardized, so repeatability is much less challenging. Processes can also be maintained and adjusted to changing organizational needs, as everyone in the department is following the documentation. Seams still exist, and different parts of the security department may not work well together.

Level 4: Advanced Maturity.
The security program has an ownership structure, with defined accountabilities for ongoing management. All parts of the security program are integrated with each other, and are mutually supporting. Data (security metrics) is collected regularly, analyzed, and acted upon. Repeatability and scalability are no serious challenge. Security forecasting becomes possible.

For more information:
solutions@ca.g4s.com • www.g4s.ca • 1-888-717-4447

Maturing Your Security Department

Robert Hastings



Level 5: Optimized Maturity. The security department is a fully integrated part of the overall organization. Security functions seamlessly work with other areas of the business. A full, formal governance structure is in place. The security program is managed continuously through established and robust QA processes. Detailed security metrics are collected on an ongoing basis, and analysis serves as a basis for continuous improvement. The management of the program is used to inform business decision-making and drive overall success of the business.

Getting From Where You Are to Where You Need to Be

It can seem a little daunting to think about how to mature your security program, especially if it seems like your program is at one of the lower levels. It's important to not be intimidated. After all, even if your program is immature, that may be fine for the organization that your security program is as part of. The first thing to know is what level of maturity your program has. The second is to know what level of maturity you need in order to meet the risk tolerance of the overall organization. Then, if you need to, you can start taking steps to mature your program.

Of course, a qualified, experienced security consultant can provide some advice and direction for this process. But however you choose to proceed with maturing your program, it is vital to have a fully-developed action plan, including project milestones, resources required at each step, and costs. The process of maturing the program must then be managed against the plan. Has the milestone been met? How much did it actually cost? What did I actually need to get it done? What is the next milestone? And so on.

The support of senior/executive managers and leaders within the organization is necessary for success. Without a higher-level commitment, it is very difficult for a security program to develop as it needs to, particularly if its maturity level is far below where it needs to be. This also serves another purpose, in that it demonstrates to the senior leadership that the security program is a true business enabler and can bring real value to the organization.

Robert Hastings, Manager, G4S Canada Risk Consulting, is a risk and physical security professional with 17 years of industry experience. Robert is a recognized expert in the area of using metrics to measure and drive security program success. His research into this area has been published in both professional and academic sources. Robert holds a bachelor's degree in Security Management from Davenport University in Michigan and a master's degree from Carleton University specializing in Infrastructure Protection and International Security. He is double board-certified by ASIS International in physical security and security management having earned both his PSP and CPP credentials. Robert is further certified as a Professional in Critical Infrastructure Protection (PCIP) through the Critical Infrastructure Institute.

For more information:
solutions@ca.g4s.com • www.g4s.ca • 1-888-717-4447