All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Duty to protect

What do you have to do and what must you not do?

One of the questions every executive should ask themselves is what their duties are. Duty to protect analysis is a process that helps you understand the nature and limitations of your duties related to protection. Not surprisingly, when you get this wrong, or fail to do it, you:

- Spend more than you have to on things that don't do what has to be done
- Spend less than you should to do the things you really should be doing.

How do I know what my duties are?

It may seem obvious, but duties derive from governance. Starting with the legal framework in which your entity exists, and working your way down through the hierarchy of sources of duties, you can identify what your duties are and reconcile your protection program with those duties. For example, for one city government we dealt with, the hierarchy ran like this:

- All relevant US, State, and County laws and regulations
- Decisions made by the City Counsel except as conflicts with above
- Orders legally given by the Mayor except as conflicts with above
- Decisions of the City Manager except as conflicts with above
- Contracts with 3rd parties, employees, and others
- External audits and findings of the auditors except as conflicts with above
- Decisions made by management except as conflicts with above
- Acts of workers authorized by the city except as conflicts with above

That's the starting point – determining the hierarchy of decision-making power as it applies to the specific situation. At the level of decisions made by managers and employees, duties may be de-facto rather than formally documented and determined, but they are duties that may be established nevertheless. For example, when a decision is made to escort employees to their cars after dark and is carried out on a regular basis, this may create a duty to do so.

Too generic?

That's the generic version of duties applied to a specific city. Of course every entity has its own governance hierarchy. And each element of the hierarchy has different specifics for different cases. Once the overall hierarchy is determined (based on reading and analyzing all relevant documents) the next step is to analyze each in context. To get you started, for a US-only company, the Federal laws relating to cyber-security (assuming you don't deal with the rest of the World) depend on the business(es) you are in. If you deal with student records, you will need to deal with FERPA, and this implies a set of regulatory requirement related to protection that you have a duty to meet. For medical records, it's the Health Information Portability and Affordability Act (HIPAA). Employee financial records, retirement funds, etc. are covered under other acts. Depending on what you have and do, your duties may differ.

At the state level, if you deal with anybody from California (US) records related to them have protection requirements related to personally identifiable information (PII) and breach notification, and lots more. County and local regulations may also apply, depending on particulars. In the US there are 50 different states plus other administrative districts, each with different laws and potential duties. And of course if you operate over the Internet, you may have to deal with international laws and laws in each country you do business with, give information to, or take information from.

Internal decision-making

Founding documents for entities typically dictate what they do and put limits on them. The form of entity combines with the legal landscape to lead to duties. Things like forming bank accounts, filing taxes, and similar acts, legal contracts, and other forms of agreements, may also involve sworn statements and content that may form contractually binding duties. The punishments associated with these dealings vary from jail for executives to fines to civil litigations, and so forth. In order to identify duties to protect, these have to be examined as well. In many cases, people sign agreements with lots of language they may not read. For example, the contracts with external providers like Google or Apple or Microsoft may create duties that are not understood within the entity or violate existing duties identified by other requirements.

Policies also create duties to protect. For example, if the company has a privacy policy, it is liable to do what the policy says in action. Failure to have a policy and carry it out surrounding things like retention and disposition can create tremendous problems in legal actions where defined duties were not carried out or duties were defined (de-facto) by individual actions resulting in unnecessary liability. One major company was fined tens of millions of dollars and the jury in a civil matter given an adverse jury instruction because of failure to have or meet a retention and disposition policy (a case of intentional spoliation of evidence). The happens at all levels of management and execution unless proper controls are in place.

Sounds really complicated

It can be really complicated, but it can be simplified in action by using systematic approaches. The approach we have found effective goes like this:

- Unless you have adequate internal expertise and resources to carry it off, hire outside experts to identify the external forces and hierarchy.
- Examine internal documentation (policies, standards, procedures, etc.) and reconcile inconsistencies. We often find that, over time, different processes produce inconsistent internal approaches and “rules”.
- Integrate duties to protect into risk management processes. This approach uses risk management to turn duties to protect into decisions about risk (acceptance, mitigation, transfer, and mitigation). It avoids undertakings not required by duties while meeting all of the duties.
- Use the management control system (typically operated by the chief information security officer or someone with appropriate related capabilities) to implement controls that meet the duties to protect but don;t exceed them.

- The management controls help set policy, standards, procedures, and other control mechanisms used to define and operate the protection program to meet the duties.
- Feedback in the controls provide the measurement and assurance that duties are met and problems identified and corrected without wasted resources.

Of course there is more to it, and the larger the entity, the more complicated it gets. But this is really no different than any other sound management process.

Translating duties into actions

In terms of what people working for the entity do, the duties to protect end up being codified into specific actions and decisions for specific workers. As the entity matures, operations go from non-existent to initial practices, they then become repeatable, documented, managed, and in rare circumstances, optimized.

The implementation of duties to protect integrate into this maturation of business processes. Processes that meet duties are initially performed and the details worked out as to how the duties will be met. A well architected approach makes this more effective and less expensive, but architecture is generally developed and adapted over time to meet changing needs. As the processes become repeatable, so do the mechanisms to carry out duties. As the processes are documented and measured, the duties are documented as are the mechanisms for meeting them. At the managed level, management uses its feedback system to assure that duties are met and adaptation is applied to make improvements and better meet duties as they change with time.

Ultimately, the duties end up codified in implementation as simple rules, often baked into procedures. For example, data retention and disposition practices may require that certain content must be retained for some number of years based on some legal or regulatory requirement, but business use may require that the content remain usable for longer. The basic rule codified into practices might read in policy as

- Data will be retained until such time as identified legal requirements, business needs, and legal holds no longer apply. When none of these requirements apply, data will be disposed of by the authorized method for the applicable data.

This policy might be applied for project XXX as a standard like this:

- Data associated with project XXX will be retained for at least 4 years since last use, 7 years since initial collection, and deleted at that time.
- Data associated with project XXX requiring special consideration for legal holds will be copied into the legal department’s retention area associated with all relevant legal matters and disposed of from that storage upon last legal requirement as defined by counsel for the specific legal matter.

The procedure based on that standard might require specific disposition practices such as:

- The database for project XXX data includes a “Creation” and “Last Use” field.
- A daily database purge will be run using the “PURGE” program to remove all data whose Creation is more than 7 years old AND Last Use is more than 4 years old.
- If Legal puts a “Hold” on data, copy the data to the “Hold” database prior to PURGE.

Of course the specifics will be dictated by the actual activities on the applicable systems, (including paper files, etc.).

These operations, in a mature system, there will also be checklists or similar methods used to make certain that, in execution, workers follow the procedures step by step and in order, and to document the process as it occurs.

This may take the form of checklists or similar methods, but in more mature environments with higher valued consequences of failure, work flow methods will be used to support the operations and confirmations of those operations taking place, including logs of activities, and reporting to upper management.

What else is needed?

In order to operate such a system, all of this should be embedded in training programs, so the workers know what do do and can do it reliably and repeatably.

Audit then has something to audit against and performance metrics for management fall out of the process as well.

The list goes on and on, depending on the nature of the duties.

Returning to the duties

This brings it all back to the duty to protect. The extent to which these duties drive other aspects of the overall protection program depends largely on the risk management process, which derives from the rewards and punishments associated with those duties.

Some duties, such as those dictated by laws like Sarbanes Oxley and the versions of this across the World, can result in top executives of public companies being put in jail for failure to carry out their duties. In one matter we dealt with, top executives a large enterprise were under judicial orders to carry out specific duties they had failed to carry out previously, and one executive went to jail for failing to do so. In another matter, the people failing properly define and carry out their duties were actually perpetrating a fraud. They too went to jail when they failed to do their duty.

In other matters, failure to carry out duties may result only in fines, negative publicity, increase liability, or other lesser punishments. In such cases, risk management may lead the enterprise to take a less certain approach to carrying out duties at lower cost. For example, companies may choose to not try to remove all copies of disposed data on all backup media because it is expensive, complicated, time consuming, and often excessive to the consequences of failure to do so. In other cases, requirement demand destruction of backup media and/or similar disposal methods. Again, this is dictated by duties and risk management.

Conclusion

Duty to protect analysis is fundamental to making good protection decisions. It can sale a lot of time and money if done well, and avoid taking excessive measures or “aiming at the wrong target”. If you haven’t looked at this issue, or don’t have a regular process for revisiting it after an initial review, you are likely either under-protecting and taking excessive risks or over-protecting and spending too much. Most likely, you are doing both – each in different areas of your protection program.

