Case Study: The Gadget Company

The Gadget Company is a Scottish, manufacturing company that designs and builds several types of gadgets. They have a sales volume of £25 million and a core base of 20 loyal customers with continuous orders and a constantly changing range of 15 – 30 customers who order only once or twice. They want to increase to 40 core customers and double the number of single orders. They have installed a new, automated Manufacturing Control System (MCS) from Vendor C to help them increase production without expanding their workforce. The company has 80 employees in several departments as shown in figure 1.

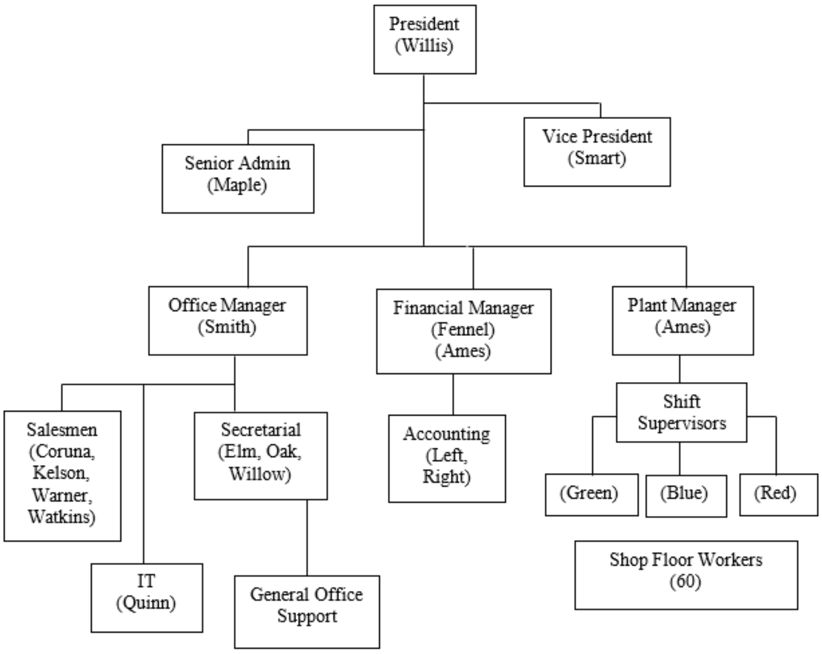

Figure 1: The Gadget Company's Organisation Chart

All customer orders come in through their salesmen. Accounting makes sure the customer has paid previous bills before the order is passed to Ames, the plant manager for production scheduling. The vice-president, Smart, is the widget designer. Requests for new designs go to him, and he works with Ames to ensure that it is something they can make. They hope the new MCS will speed up this process. They don't have more than a basic Web site yet, but they are seriously considering building one that core customers can use to place repeat orders and that new, potential customers can use to see what types of new widget designs they have.

Each shift supervisor coordinates with Ames to see what production runs are required for the shift. The shift supervisors are responsible for scheduling during their shifts and coordinating with the follow-on supervisor in case of delays. The new MCS requires training to use, so the shift supervisors and some of the staff floor workers have had some training. They will be evaluating their progress in four months to determine if they want to add a second automated production line. The salesmen are under pressure to increase their sales to use the automated system to capacity. They have a recently hired IT person (Quinn) to help them with their rapidly increasing computer support. They previously relied on whoever in the office understood computers and a third-party service provider (Vendor B).

The Gadget Company's competitive edge has always been their customer service, the high quality of their gadgets, their ability to build custom-designed widgets, their ability to rapidly produce high volumes of gadgets, and being the only company of its kind in Scotland.

However, recently, a competitor opened up with a fully automated factory floor. They make other things besides gadgets, but they also have the capacity to produce high-quality, high volumes of gadgets at lower prices. They have the potential for cutting into the Gadget Company's customer base.

With the new competitor, maintaining their competitive edge has become critical to their survival.

1. Asset Information:

MCS, a new manufacturing control system – Vendor C developed the manufacturing control system and supports it 24/7, although it is currently used only during the first and some of the second shift and runs in parallel with the older manual manufacturing system. Vendor C must respond to any problem with the system within 4 hours. The vendor set up email capability to communicate with the shift supervisors and a Web server to store the latest version of the control system's documentation. The vendor accesses email from the shift supervisors using a direct dial-in line to the Gadget Company control system server. The vendor can also remotely upgrade the production software and the Web-based documentation for the control system.

COTS (commercial-off-the-shelf) personnel database – This database is managed by the Gadget Company administration. The personnel database stores all personnel information, including salary, benefits, disciplinary actions, workman's compensation records. The personal computers (PCs) that access the database sit in open cubicles. The database is on Server 2, but is accessible only by managers. This hardware and software are supported through a maintenance contract with Vendor B.

Office System – This system includes the managers' PCs, the administrative PCs, two servers, and the network. It also includes a lot of software for the inventory, financial records, electronic gadget designs, word processing, spreadsheets, email, etc.

Managers' PCs – All senior managers and shift supervisors have networked PCs that contain strategic and operational plans, conceptual and design documents for proposed new gadgets, and customer information (orders and shipments). The master copy of all data is kept on a separate server (Server 2) from the email and Web site (Server 1). Vendor B used to maintain the managers' PCs and server, but the new IT person (Quinn) has taken that over.

Administrative PCs – These have access to all personnel records, gadget design specifications, customer records, and all servers except for the one used with the new MCS.

Mobile devices and home PCs – All of the managers, salesmen, and the senior administrative assistant have home PCs that link into the company's office computer system. They also have personal mobile devices that can download schedules and other types of information so that everyone can remain up-to-date while on the road.

Plant architectural drawings, designs, and maintenance records – These records are a collection of paper files kept in a drawer in the president's office. These also include the specifications for the security system, physical layout, and the upgrades built to handle the increased automation.

Gadget design specifications – Each type of gadget has its own specific design, documented in both paper and electronic documents. The electronic versions of the designs are translated into special input format by Vendor C for the MCS. There are 12 basic designs and 23 variations. These designs are referred to in customer order documents by their unique reference number. Only 7 of the basic designs have been converted for the MCS.

Customer records – The customer orders are called or emailed in by salesmen to two of the administrative staff, who rotate order-taking duties with general office support. The customer records reside on a server accessible by all administrative and manager workstations (Server 1).

Financial records – Accounting keeps a set of records for all contracts, billing, receipts, taxes, loans, salaries, etc. These records reside on Server 2 and have been encrypted by the new IT person (Quinn). Quinn, the two accountants, and the office manager can encrypt/unencrypt files.

Production schedules – Based on the customer requests and the plant manager's shift assignments, all shift supervisors set up the production schedules for their shifts on a weekly basis. Some adjustments are made as needed for overruns or unexpected delays. Schedules are either paper or electronic, based on the preference of the shift supervisor.

Inventory – Additional gadgets are stored in the back corner of the shop floor. They keep a backlog of the standard set of gadgets at all times. New designs are made only when requested. The inventory is kept on Server 2 and is managed jointly by the office administrative personnel, accountants, and plant manager.

2. General information about some key personnel:

Job Title	Name	Responsibilities	Background and Other Information
President	P. Willis	Long-range planning, external interfaces, overall management, customer interface (the personal touch)	Started this company in his garage with J. Smart. Primarily interested in continuing to expand the company and increase profit margin. Keeps in personal contact with core customers and investors, and handles the customer interface part of special orders. Plays a lot of golf.
Vice President	J. Smart	Oversight of day-to-day operations across shop floor and office; design of new gadgets; hiring and termination	Technically savvy and up-to-date with computers. Responsible for bringing in the MCS and hiring a full-time IT person. Worried about information security. Does all of the new design specifications and special orders. Starting to work with Quinn on security issues.
Office Manager	M. Smith	Manages all office supply and non-shop floor purchasing and the cleaning contractor. Manages all office personnel	Was not too happy about the new IT person. Quinn was hired over her objections. Wanted the responsibility and saw it as an opportunity for learning and expansion that's now lost. Now recognizes that there is a lot to learn and is trying to help Quinn.
Plant Manager	J. Ames	Creates master production schedule for each week based on customer orders and inventory; works with Smart to ensure new designs are feasible	Very knowledgeable in design and production of gadgets. Moved up in the company from shift supervisor. Enthused about MCS. Has been concerned about the increasing numbers of specialty design orders and the time it takes to verify new designs. Keeping an eye on the mood of the shop floor workers as everyone settles in with MCS.
Financial Manager	G. Fennel	Manage budgets, finances, and contract reviews. Approval and signature on all contracts.	Promoted 2 years ago from an accountant to manage Gadget Company's growing financial work. Took over budgets from Smart.
Shift Supervisor	L. Green	First shift management – schedules gadget runs and personnel; manages the new automated system	Trying to work with other shift supervisors to move more production runs to first shift now that the automated system is freeing up more people to work on the older equipment.
Shift Supervisor	T. Blue	Second shift management	Has learned the newer equipment and is starting to use it for limited production runs on his shift. Not willing to move any of the runs to first shift.
Shift Supervisor	S. Red	Third shift management	Has the least seniority (only on the job two months) and is the most likely to see his production runs moved to the other shifts. Very worried about the job; got promoted suddenly when the former shift supervisor left for the rival across town.

Job Title	Name	Responsibilities	Background and Other Information
IT	A. Quinn	Maintains office computers and applications; serves as the interface with vendors; manages phone system and other office equipment	Very new – was hired only three months ago. Straight out of university with a degree in information technology with a few security-related courses. Really wants to train people on computers and their applications and improve security. Too new to know the right way to go about getting approval for upgrades. Rapidly becoming irreplaceable.
Salesman	H. Coruna	Customer contact, contract generation, sales	Been with the company seven years and does not use the laptop for anything other than browsing the Internet and sending email. Carries paper and glossy sales materials and specifications and phones the orders in, usually to A. Elm.
Salesman	I. Warner	Customer contact, contract generation, sales	New but very enthusiastic. Keeps up with technology and keeps all of the customer information close at hand on the laptop and PDA. Constantly networked back to the main office. Sends orders by email. Likes to show customers the latest gadget specifications to close the deals.
Accountant	S. Left	Salary and budget administration	An accountant with six years of experience, all with this firm. Has access to all personnel and financial information, including customer order data. Computer savvy, but has trouble remembering passwords.
Sr. Administration	L. Maple	Coordinates and manages all administrative staff. Manages Mr. Willis's schedule and work	Willis's and Smart's personal assistant, has been with the company for 10 years. Nothing gets done in the business offices without Maple's oversight. Maple has access to all files and all rooms.
Administration	A. Elm	Takes orders from salesmen, some customer interface, and manages the insurance claims and procedures	A former temporary employee, now full-time for about a year. Eager to learn everything, has volunteered to learn all of the systems and databases and has been learning as much as possible from Quinn about the networks and computers. Very computer savvy.
Senior Shop Floor Worker	D. Ash	First shift worker, can work on all of the different gadgets but is only partly trained on the new automated system	Has 20 years in this company. Been here from the beginning. Loyal but worried about the future. Very leery of new technology. Not computer-savvy.
Shop Floor Worker	P. Smithers	First shift worker, can work on all of the different types of gadgets. Has learned to work with the automated system	Has 10 years with this company. Would like to move up to second shift supervisor. Keeps up with advances in related technology and has a computer at home.

Job Title	Name	Responsibilities	Background and Other Information
Shop Floor Worker	E. Beggs	Third shift worker, works on most of the different types of gadgets. Has not learned the automated system yet	Has two years at this job, does not intend for this to be a career, but needs to save money for university.
Shop Floor Worker	O. Moore	Second shift worker, works on the most commonly ordered gadgets, and is learning to work on the rest. Has learned to work with the automated system	Has four years at this job, a new family to support, and is very concerned about the automation and what it means to his job.

3. Current practices of the company:

The following tables summarise survey and personnel interview information for each area of practice. Areas of practice are categorised into (i) **Strategic Practices** (SP), and (ii) **Operational Practices** (OP). The information for each area is provided in two tables. First, a summary of the answers to the survey questions from each level of the organization is provided. Then, individual comments from each level relative to the area are provided. The comments may sometimes contradict the survey answers. Remember that each comment is from a single person while the summary of the answers is from a much broader selection of personnel. For example, if one person is unaware of policies, it may be because that person is new, forgot, or it could be an indicator of inconsistent communication.

The following legends apply to the contents of the tables:
Legend
As perceived by personnel at this level:
yes – The practice is most likely used by the organization.
no – The practice is most likely not used by the organization.
unclear – It is unclear whether the practice is present or not.
blank – The question was not asked of this level.

Criteria:
Yes: 75% or more of respondents replied yes.
No: 75% or more of respondents replied no.
Unclear: Neither the yes nor no criteria were met.

Security Awareness and Training (SP1): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
Staff members understand their security roles and responsibilities. This is documented and verified.	Unclear	Unclear	No	No
There is adequate in-house expertise for all supported services, mechanisms, and technologies (e.g., logging, monitoring, or encryption), including their secure operation. This is documented and verified.	Unclear	Yes	Unclear	No
Security awareness, training, and periodic reminders are provided for all personnel. Staff understanding is documented and conformance is periodically verified.	Unclear	No	Unclear	No

Security Awareness and Training (SP1): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management	Quinn did start awareness training for everyone.	Not everyone's had Quinn's briefing and it's only a start at training. Only Quinn and Smart know what their roles and responsibilities are.
Operational Area Management	We did attend some training from Quinn. Not sure the scope was adequate.	
Staff	Some people had some training from Quinn.	Not all of us could attend the training. We know we're not supposed to share passwords, but there are probably other things we're supposed to do. We need something written as a reminder of our responsibilities.
IT Staff		The awareness training was incomplete and not taken by everyone. Very few have any idea what their role is. As the sole IT staffer, I know I need a lot more training.

Security Strategy (SP2): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
The organization’s business strategies routinely incorporate security considerations.	Unclear	Unclear		
Security strategies and policies take into consideration the organization’s business strategies and goals.	Yes	Unclear		
Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization.	Unclear	No		

Security Strategy (SP2): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management	Security strategy, such as it is, does consider our business goals. There’s just not a lot of strategy.	Business strategy doesn’t consider security, except perhaps on an individual basis, like Smart.
Operational Area Management		If there’s a security strategy, we haven’t seen it so we don’t know what it takes into consideration. Don’t have any idea if the business strategy considers security but with Smart’s expertise, surely it does. We just don’t know for sure.
Staff		
IT Staff		

Security Management (SP3): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
Management allocates sufficient funds and resources to information security activities.	Unclear	Yes	Yes	No
Security roles and responsibilities are defined for all staff in the organization.	Unclear	Unclear	Yes	No
The organization's hiring and termination practices for staff take information security issues into account.	Unclear	Yes	Yes	No
The organization manages information security risks, including • assessing risks to information security • taking steps to mitigate information security risks	No	Unclear	Unclear	No
Management receives and acts upon routine reports summarizing security-related information (e.g., audits, logs, risk, and vulnerability assessments).	Unclear	Unclear		Yes

Security Management (SP3): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management	We thought we had enough funding allocated. Budget and scheduling risks we manage.	Maybe we do need more funds. This evaluation should tell us that. We never even considered security before in terms of firing.
Operational Area Management	We hired Quinn.	Not sure what managing security risks means. Don't know if there are reports about security much less if anyone sees them. Security isn't in the budget, but it should be.
Staff		They never fired that temp who got into the personnel files. What's security risk management?
IT Staff	I get several reports and vendor B also provides reports. Smart reviews and acts on them	We desperately need more funding and need consider how much at risk we are.

Security Policies and Regulations (SP4): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
The organization has a comprehensive set of documented, current policies that are periodically reviewed and updated.	Unclear	Unclear	Unclear	No
There is a documented process for management of security policies, including • creation • administration (including periodic reviews and updates) • communication	No	Unclear	Unclear	No
The organization has a documented process for evaluating and ensuring compliance with information security policies, applicable laws and regulations, and insurance requirements.	Yes	Yes	Unclear	Yes
The organization uniformly enforces its security policies.	Yes	Yes	Yes	Unclear

Security Policies and Regulations (SP4): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management	We have some policies that Smart wrote and keeps current. Other types of regulations and laws (not security) we have long standing policies and processes for insuring compliance.	We use an informal, not a documented process to manage policies.
Operational Area Management	We comply with many regulations. Several polices have been documented. Maybe they should be a part of training	If there are security regulations, we may not track compliance. I've never seen these policies.
Staff		
IT Staff		There's no enforcement of security policies at the moment.

Collaborative Security Management (SP5): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
The organization has policies and procedures for protecting information when working with external organizations (e.g., third parties, collaborators, subcontractors, or partners), including • protecting information belonging to other organizations • understanding the security policies and procedures of external organizations • ending access to information by terminated external personnel	Unclear	No	Unclear	No
The organization has verified that outsourced security services, mechanisms, and technologies meet its needs and requirements.	Unclear	Unclear		No

Collaborative Security Management (SP5): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management	We made sure that both vendors know what we need. Smart has an informal working relationship with Vendor C.	There's some doubt now that we knew what we needed when we signed those contracts. Not sure how we'd verify this.
Operational Area Management		
Staff		
IT Staff	Vendor B informally works with Quinn to help him with patches and administrative tools.	There's no real verification that they actually do what we ask.

Contingency Planning/Disaster Recovery (SP6): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
An analysis of operations, applications, and data criticality has been performed.	Yes	Unclear		Yes
The organization has documented, reviewed, and tested • business continuity or emergency operation plans • disaster recovery plan(s) • contingency plan(s) for responding to emergencies	Yes	Yes		Yes
The contingency, disaster recovery, and business continuity plans consider physical and electronic access requirements and controls.	No	Unclear		No
All staff are • aware of the contingency, disaster recovery, and business continuity plans • understand and are able to carry out their responsibilities	Yes	Yes	Yes	Yes

Contingency Planning/Disaster Recovery (SP6): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management	We do have disaster recovery plans and everyone knows about them. We have fire and flood insurance. This evaluation is our data analysis.	Those plans do not consider computer security.
Operational Area Management	The plans exist. OSHA requires an evacuation plan.	Most of us have seen them, but not all
Staff	I’ve seen the plans and I know the administrative staff knows what to do.	I’m sure we have them, but I’ve never seen them and I’m not sure what I’m supposed to do.
IT Staff	Plans for the usual disasters exist.	Lack of contingency plans if the network stays down or we lose the servers

Physical Security Plans and Procedures (OP1.1): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
Facility security plans and procedures for safeguarding the premises, buildings, and any restricted areas are documented and tested.	Yes	Yes	Unclear	Yes
There are documented policies and procedures for managing visitors.	Yes	Yes	Yes	Yes
There are documented policies and procedures for physical control of hardware and software.			Yes	Unclear

Physical Security Plans and Procedures (OP1.1): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management	We have the policies and procedures. Vendors keep a visit log for billing purposes.	We don’t test them very often and we’re a bit weak on enforcement.
Operational Area Management	Visitors must be signed in and accompanied at all times on the shop floor.	Physical security is just too lax in the office. It’s better on the shop floor, but it’s not as good as it could be.
Staff	Everyone is supposed to lock their office doors; L. Maple has keys to all of them.	There are areas in the office suite that should be controlled and aren’t.
IT Staff		Disks are not controlled at all. Software is partially controlled.

Physical Access Control (OP1.2): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
There are documented policies and procedures for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media.	Unclear	No	Unclear	Unclear
Workstations and other components that allow access to sensitive information are physically safeguarded to prevent unauthorized access.	No	Yes	No	No

Physical Access Control (OP1.2): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management		I don’t think we do any of this, but I’m not really sure.
Operational Area Management	The managers keep their office doors locked on off hours so those areas are controlled.	There’s no control – we can get to any office machine.
Staff	I remember being given procedures for this but I can’t remember where they are.	The only control is a password, and those aren’t always a secret.
IT Staff		No one’s let me put any controls in yet. Maybe they will after this evaluation.

Monitoring and Auditing Physical Security (OP1.3): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
Maintenance records are kept to document the repairs and modifications of a facility's physical components.		Yes		Yes
An individual's or group's actions, with respect to all physically controlled media, can be accounted for.		Unclear		No
Audit and monitoring records are routinely examined for anomalies, and corrective action is taken as needed.		Yes		Unclear

Monitoring and Auditing Physical Security (OP1.3): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management		
Operational Area Management	There are monthly reports on maintenance/repairs of all equipment, both shop floor and office.	Don't think we track individual activity
Staff		
IT Staff	We track repairs and modifications.	There's no way, currently, to track an individual's actions. The audit records aren't really that good – too simple, too spotty. We need better ones.

System and Network Management (OP2.1): Survey Results

Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
There are documented and tested security plan(s) for safeguarding the systems and networks.	Unclear	Unclear		Yes
Sensitive information is protected by secure storage (e.g., backups stored off site, discard process for sensitive information).				No
The integrity of installed software is regularly verified.				Unclear
All systems are up to date with respect to revisions, patches, and recommendations in security advisories.				Yes
There is a documented and tested data backup plan for backups of both software and data. All staff understand their responsibilities under the backup plans.	Unclear	Unclear	No	No
Changes to IT hardware and software are planned, controlled, and documented.				No
IT staff members follow procedures when issuing, changing, and terminating users' passwords, accounts, and privileges. • Unique user identification is required for all information system users, including third-party users. • Default accounts and default passwords have been removed from systems.				Yes
Only necessary services are running on systems – all unnecessary services have been removed.				Unclear

System and Network Management (OP2.1): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management	We have the plans, the vendors wrote them and we approved them.	We don’t test them.
Operational Area Management	We back up the financials	Don’t think all the designs are backed-up.
Staff		
IT Staff	Vendor B gave me a good set of procedures to follow for user passwords and all. I follow those. I patch everything at the same time.	Back-ups are not complete, even for critical information. I occasionally check the integrity of the software, but I just don’t have the time to do all of it. I can’t control people making changes after I update and verify their systems and laptops.

System Administration Tools (OP2.2): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
Tools and mechanisms for secure system and network administration are used, and are routinely reviewed and updated or replaced.				Unclear

System Administration Tools (OP2.2): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management		
Operational Area Management		
Staff		
IT Staff		Vendor C may do this for MCS, but we can’t verify that. I do some of this for the office system, and Vendor B may be doing some remotely, but we can’t verify that.

Monitoring and Auditing IT Security (OP2.3): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
System and network monitoring and auditing tools are routinely used by the organization. Unusual activity is dealt with according to the appropriate policy or procedure.				Unclear
Firewall and other security components are periodically audited for compliance with policy.				Unclear

Monitoring and Auditing IT Security (OP2.3): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management		
Operational Area Management		
Staff		
IT Staff		It’s just not clear what the vendors are doing with MCS and the office systems. I’m not doing very much for the office system.

Authentication and Authorization (OP2.4): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
Appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to information, sensitive systems, specific applications and services, and network connections.		Unclear		No
There are documented policies and procedures to establish and terminate the right of access to information for both individuals and groups.	Yes	Yes		No
Methods or mechanisms are provided to ensure that sensitive information has not been accessed, altered, or destroyed in an unauthorized manner. Methods or mechanisms are periodically reviewed and verified.				No

Authentication and Authorization (OP2.4): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management		
Operational Area Management	Financials are somewhat controlled There are some procedures documented somewhere. I've seen them.	I have access to too much – there's no consistent control. Everyone can get to everything, except financial. They can get to financial too, if they really tried.
Staff		
IT Staff	There are some minor controls on access to financial data.	What policies exist aren't documented and usually are not consistently followed. I just don't have the time to keep up as much as I should. I didn't get around to canceling the summer interns' accounts for a few months after they left. I was just encrypting financials.

Vulnerability Management (OP2.5): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
There is a documented set of procedures for managing vulnerabilities, including • selecting vulnerability evaluation tools, checklists, and scripts • keeping up to date with known vulnerability types and attack methods • reviewing sources of information on vulnerability announcements, security alerts, and notices • identifying infrastructure components to be evaluated • scheduling of vulnerability evaluations • interpreting and responding to the results • maintaining secure storage and disposition of vulnerability data				No
Vulnerability management procedures are followed and are periodically reviewed and updated.				Unclear
Technology vulnerability assessments are performed on a periodic basis, and vulnerabilities are addressed when they are identified.				Yes

Vulnerability Management (OP2.5): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management		
Operational Area Management		
Staff		
IT Staff	I do some, on my own, with help from Vendor B.	We don’t do this formally. There’s no documented procedure. The vendors are supposed to do this and they might. But we don’t know for sure.

Encryption (OP2.6): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
Appropriate security controls are used to protect sensitive information while in storage and during transmission (e.g., data encryption, public key infrastructure, virtual private network technology).				Unclear
Encrypted protocols are used when remotely managing systems, routers, and firewalls.				Yes

Encryption (OP2.6): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management		
Operational Area Management		
Staff		
IT Staff	Some data is protected (financials). No other data has been identified as critical to protect in this way.	

Security Architecture and Design (OP2.7): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
System architecture and design for new and revised systems include considerations for • security strategies, policies, and procedures • history of security compromises • results of security risk assessments				Unclear
The organization has up-to-date diagrams that show the enterprise-wide security architecture and network topology.				Yes

Security Architecture and Design (OP2.7): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management		
Operational Area Management		
Staff		
IT Staff	I have the latest maps and diagrams from Vendor B. In fact, I let them know if I change anything so they can keep up to date.	We haven’t really updated anything so it hasn’t occurred so far.

Incident Management (OP3.1): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
Documented procedures exist for identifying, reporting, and responding to suspected security incidents and violations.	Unclear	Yes	Unclear	No
Incident management procedures are periodically tested, verified, and updated.	No	Unclear	Unclear	No
There are documented policies and procedures for working with law enforcement agencies.	Unclear	Unclear	No	No

Incident Management (OP3.1): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management	We have informal arrangements with the local police.	There's nothing documented for any of this, much less tested.
Operational Area Management	We have documented procedures for the usual crimes.	Surely Smart and Quinn have dealt with this. But we don't actually know anything about it.
Staff	President Willis is on very good terms with the Chief of Police. They'd come right away if we had any trouble.	
IT Staff		The vendors actually gave me copies of standard procedures for dealing with incidents. I've never used them. The other procedures and polices don't exist, as far as I know.

General Staff Practices (OP3.2): Survey Results				
Survey Statement	**Senior Managers**	**Operational Area Managers**	**Staff**	**IT Staff**
Staff members follow good security practice, such as • securing information for which they are responsible • not divulging sensitive information to others (resistance to social engineering) • having adequate ability to use information technology hardware and software • using good password practices • understanding and following security policies and regulations • recognizing and reporting incidents	Unclear	Yes	Unclear	No
All staff at all levels of responsibility implement their assigned roles and responsibility for information security.	Unclear	Yes	Yes	Unclear
There are documented procedures for authorizing and overseeing all staff (including personnel from third-party organizations) who work with sensitive information or who work in locations where the information resides.	Unclear	Unclear	Unclear	Unclear

General Staff Practices (OP3.2): Contextual Information		
Organizational Level	**Protection Strategy Practices**	**Organizational Vulnerabilities**
Senior Management	Everyone can be trusted to keep the success of this company in mind. We don't need formality	We really have gotten quite lax about passwords and laptops keeping even paper-based designs secure. We don't have defined roles so they're not being followed.
Operational Area Management	I've talked with Quinn about formalizing staff procedures.	I don't think there are procedures for overseeing people using critical data. We need better staff practices with rewards or incentives.
Staff	We follow most of the rules.	We do share passwords. It's just more convenient.
IT Staff		People like to think they're following the rules, but they rarely do.

4. Business Impact Analysis and Evaluation Criteria

Evaluation Criteria			
Impact Area	**High**	**Medium**	**Low**
Reputation/ Customer Confidence	• 6 or more of our competing customers lose confidence in our ability to keep their information secret • Lose 2 or more customers • Delay charges for 4 or more customers • 1 or more customers sue for damages from incorrect gadgets, delays, etc.	• 2-5 of our competing customers lose confidence in our ability to keep their information secret • Lose 1 customer • Delay charges for 1-3 customers	• 1 of our competing customers loses confidence in our ability to keep their information secret • President has to personally contact customers and convince them to stay with us • Minor customer delays (less than 1 week on normal orders)
Employee Safety	• Loss of life or irrecoverable injury • Large number of recoverable injuries (more than 6 shop floor or staff) • Lawsuit by 1 or more employees	• Recoverable injury, some downtime for employee(s) (1-48 hours) • Threat of lawsuits, out-of-court settlement of less than £50,000 (covered by insurance policy)	• Use of on-site first aid
Productivity	• Loss of 13 or more hours of production runs per week • Union-organized strike • Employee turnover on shop floor of more than 15% per quarter	• Loss of 5-12 hours of production runs per week • Unofficial “slow-down” • Both accountants out sick during peak financial periods (taxes, inventory) • Employee turnover on shop floor of 5-15% per quarter	• Loss of 0 – 4 hours of production runs per week • Up to 3 shop floor workers from the same shift, and up to 2 administrative workers out sick at the same time • Employee turnover on shop floor of 0-5% per quarter
Fines/ Legal Penalties	• Audit penalty over 5% of sales • Negative HSE finding requiring retraining or measures that cost more than 5% of sales	• Audit penalty of 0-5% of sales • Negative HSE finding requiring retraining or measures that cost 0-5% of sales	• Negative audit finding • Negative HSE finding that can be corrected through procedural or paper changes
Financial	• One-time loss of more than £200,000 (exceeds insurance policy)	• One-time loss of £50,000 to £200,000 • Recurring costs or losses from £2000-6000/month	• One-time loss of less than £50,000 • Recurring costs or losses up to £2000/month

<table>
<tr><th colspan="4">Evaluation Criteria</th></tr>
<tr><th>Impact Area</th><th>High</th><th>Medium</th><th>Low</th></tr>
<tr><td></td><td>• Recurring costs or losses above £6000/month</td><td></td><td></td></tr>
</table>