Enterprise Threat Assessment

In this exercise we perform a threat assessment upon a hypothetical enterprise: a small internet-based desktop publishing company that prints business cards and advertising material for small businesses. We create a hypothetical list of possible information assets possessed by such a company, enumerate threat sources and actors that might have a motivation to gain access to those assets, and explore possible compromise methods for a hypothetical infrastructure for the enterprise.

We make a number of assumptions about this enterprise in order to assess the relevant threats:

- The enterprise hosts a relatively well known proprietary web application using its own servers.
- The web application is connected to a back-end that automates the printing process without need for human intervention.[1]
- The enterprise owns its own printing equipment but contracts another company for maintenance.
- The enterprise employs its own small network administration team.

We have used the HMG1 standard as a guide for our threat assessment. This standard is applicable to the threat assessment of real businesses and so we believe it to be suitable for our hypothetical scenario.

We have identified the following information assets for our hypothetical enterprise:

- Strategy – Future plans for expansion, diversification or acquisition of other companies
- Products and Services – Printed business cards, advertising material and other documents produced for small businesses
- Intellectual Property – Licensed artwork and designs
- Projects – Records of batches of printing scheduled to take place, or which has recently been completed
- Training Materials – Information on equipment specifications and operating procedures
- Marketing Media – Upcoming promotions or prices, sales portfolio
- Customer Lists – All consumers who have used the services and possibly will interact with the company in the future
- Operations – Software operations (Web server and interface), Printing operations, intra-company communication procedure
- Financial – Employee wages and expenses, purchasing data from customers
- Organizational Culture – Procedure strictness, customer interaction procedure
- Legal and Compliance – Data protection regulations, Performance reviews

[1] https://web.archive.org/web/20080513052250/http://www.printaction.com/default.php/online/interview_Paul_Tasker

GTB984, KNM986, DXD946

Threat Sources and Actors

In order to fully assess the threats to our enterprise we have enumerated a list of possible threat sources and actors along with their motivations, possible deterrents, and their technical capabilities. These factors each affect the type of attack that the threat can launch and the vectors by which they are likely to do so; the relevant deterrents are helpful in devising appropriate defences for each of these vectors.

Some of these threats can be classified as both a source or an actor. For the majority of cases we have not separated threats along these lines; our exploration of actors tended to show that:

- The motivation of actors tends to be the same (financial, through bribes or blackmail), and
- The capability of actors is typically increased by the same means (provision of malicious software or equipment by the threat source).

Actors/Sources	Type	Motivations/Deterrences	Capability
Cleaner	Bystander (BY)	**Motivated by:** • Monetary gain from eg. bribes • Personal gain by direct theft • Minimal career prospect impact • May be disgruntled with company **Deterred by:** • Threat of criminal conviction • Physical site security ◦ Locks and visible alarms / signage ◦ CCTV • Authentication on workstations	**Low** – Can introduce malicious content developed by a third party using a removable device or to physically steal items. Usually has no personal logical access however may have acquired credentials illegitimately
Printer Maintenance Contractor	Service Provider (SP)	**Motivated by:** • Acquiring Strategy information assets to inform production priorities • Knowledge on future purchases **Deterred by:** • Legal repercussions if caught • Don’t wish to ruin business relationship	**Med** – Has the capability of introducing backdoors into equipment or other hardware solutions
Print Engineer (Acting for Print Maintenance Contractor)	Handler (HAN)	**Motivated by:** • Approval or increased standing with Print Maintenance Contractor • Salary increases from employer **Deterred by:** • Loss of trusted position if caught • Negative reputation ruins future employment prospects	**Med -** Has significant knowledge of hardware and would be able to cause significant damage to the company infrastructure. Active but cautious as does not want to bring themselves or the company into disrepute.
Print Engineer (Source)	Handler (HAN)	**Motivated by:** • Acquisition and sale of sensitive data • Personal gain from theft of equipment • Perceived mistreatment by our company **Deterred by:**	**Med/High -** Has significant knowledge of hardware and would be able to cause significant damage to the company infrastructure.

GTB984, KNM986, DXD946

		• Physical site security
		  ◦ Locks and visible alarms / signage
		  ◦ CCTV
		• Negative reputation ruins future employment prospects	

Customer Support	Normal User (NU)	**Motivated by:** • May be disgruntled with company • Bribed / Blackmailed by 3rd party **Deterred by:** • Loss of employment • Threat of criminal conviction • System monitoring and logging by administrators • Restricted access to non-relevant information	**Med** – Has limited access to the system, however does not have administrative access. Potentially has access to sensitive customer details that could be used for further exploits. If improperly trained could leak sensitive data unintentionally.

Web Service Administrator	Privileged User (PU)	**Motivated by:**
		• Feeling of ownership over application
		  ◦ Using web platform for personal use or gain
		  ◦ Disagreement with system policy decisions
		• May be disgruntled with company
		• Bribed / Blackmailed by 3rd party
		• Desire to demonstrate their technical capabilities (Show-off)
		Deterred by:
		• Automated system monitoring and logging, possibly off-site or to cloud where it cannot be accessed by the administrator
		• Enforced removable device policy
		• Data transfer restrictions applied to eg. company email service
			High – Admin access. Implemented security systems and base application. Would have the company's technical resources at their disposal. Good theoretical knowledge of systems. In a trusted position so likely to be exempt from some monitoring.

Stationary Supplier	Supplier (SUP) / Information Exchange Partner (IEP)	**Motivated by:** • Bribed / Blackmailed by 3rd party • Prediction of future requirements that can be fulfilled for economic gain **Deterred by:** • Quality control checks on receipt of supplies • Legal and respect repercussions if caught	**Low** – Unlikely to have many technically trained staff / specialist equipment. Could sabotage / tamper supplies to damage equipment and reputation of company.

Script Kiddie	Indirectly Connected (IC) / Person Within Range (PWR)	**Motivated by:** • Showing off • Entertainment • Testing or improving their skills • Payment by 3rd party • Personal vendetta against company, or companies that share characteristics with ours. **Deterred by:** • Frequent application of security patches • Threat of criminal conviction • Obvious presence of security upon remote access • Multiple security layers	**Med** – Have access to freely available tools that may compromise the network. They have a low understanding of scripts but enough knowledge to implement them.

Thief	Physical Intruder (PI)	**Motivated by:**
		• Payment by 3rd party
		• Gain access to sensitive data to sell / pass on
		• Disgruntled by or personal vendetta against company.
		Deterred by:
		• Threat of conviction
		• Physical site security
		  ○ Locks and visible alarms / signage
		  ○ CCTV
		  ○ “No tailgating” policy
		• Concealing desirable equipment
			Low – low technical sophistication. However, don't need high technical ability to steal

Customer	Service Consumer (SC)	**Motivated by:** • Identification of their competitors using our service • Reducing charges they receive for using service or increasing volume of product they receive. • Other actors may pose as legitimate customers **Deterred by:** • Criminal conviction • Obvious security measures	**Low** – unlikely to have specialist equipment or technical ability, but does have access to a legitimate account with the business.

Actor using same ISP	Shared Service Subscriber (SSS)	**Motivated by:** • Competitive advantage • Disgruntled by company • Bribes/Blackmail from 3rd party **Deterred by:** • Threat of criminal conviction • Visible alternative means of hosting web service	**High** – must have the capability to cause disruption to a large, well-secured network provided by the ISP.

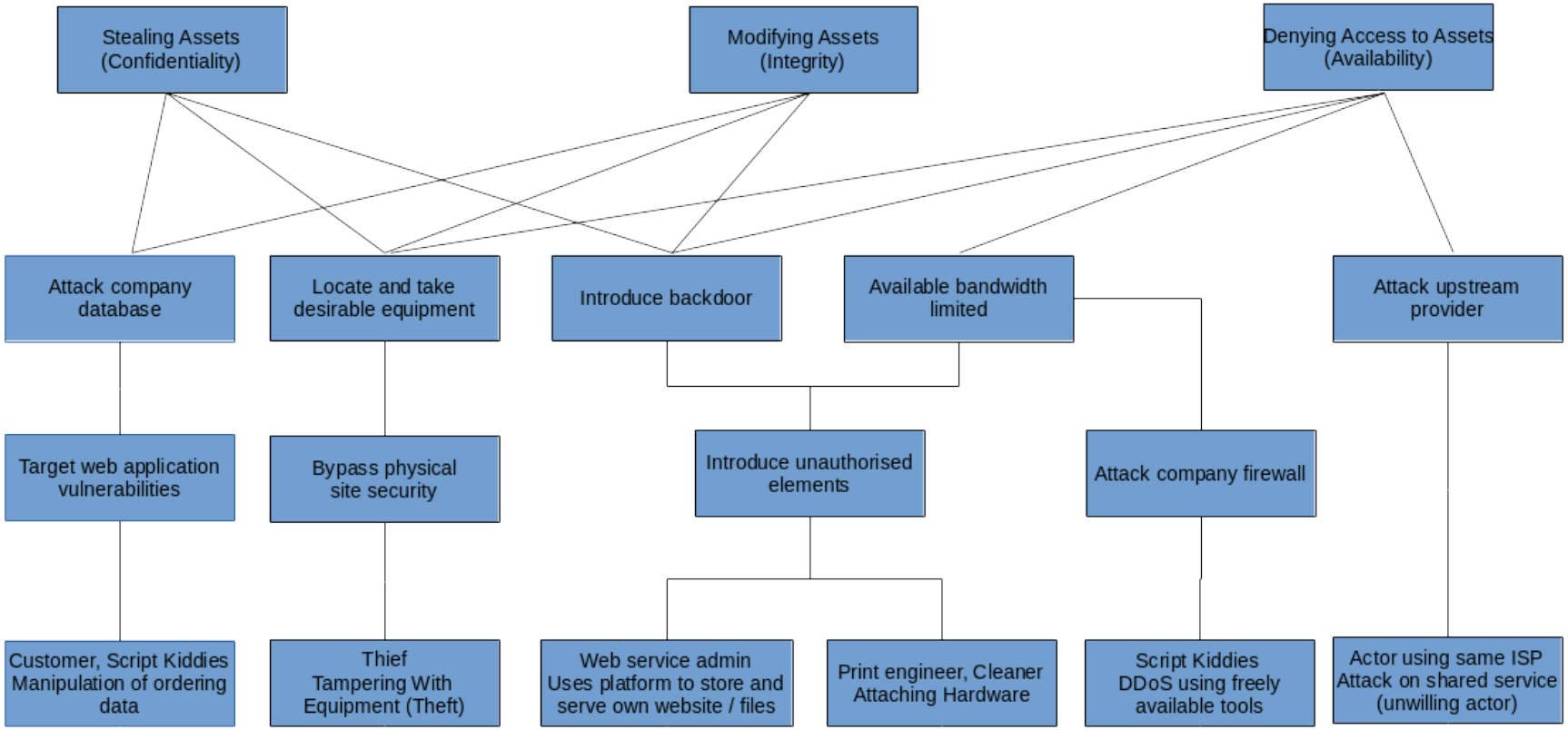
Compromise Methods

We have selected several of our identified threat sources and actors, and have considered some methods by which they might achieve their goals. We have considered the impact of these attacks in terms of breaches of confidentiality and integrity, and in terms of threats to the availability of the company's services. From this we have constructed an attack tree for these specific threats.

Compromise method	**Source/s**	**CIA area/s under threat**	**Possible resolutions/ reductions to damage**
1. Misuse of Network connections (DDOS Attack solely to overload servers)	Script Kiddies	A	Using Load balancing and IP banning together Use a cloud-based service that can pool more resources
2. Tampering with equipment (Attaching hardware)	Cleaner, Print Engineer	CIA	Checking for devices on the actors person before allowing entry Covering unused ports and buying lock in cables for those that aren't Set up software countermeasures that stops unauthorised port use/changes
3. Tampering with equipment (Theft)	Thief	CIA	Create layers of security to depend, making sure to vary types of defence Separate important equipment in multiple locations
4. Changes the Configuration (Uses platform to store and serve own website or file storage)	Web Service administrator	A	Psychological evaluations of staff Monitoring of employees after disciplinary action Regular Auditing of Security systems
5. Misuses Business or Network connections (Manipulation of ordering	Customer, Script Kiddies	CI	Prepared statements or input sanitization Using well established libraries

data)			Banner declaring prosecution policy Strict access permissions (reduce surface area of attack)
6. Misuses Business or Network connections (Attack on shared service)	Actor using same ISP (Unwilling Actor)	A	Redundant Servers off-site or on alternative platforms Special selection of ISP based on their resilience

Attack Tree



GTB984, KNM986, DXD946