INFORMATION SYSTEMS SECURITY ASSESSMENT

OF

RACCOON CITY POLICE DEPARTMENT'S SPECIAL TACTICS AND RESCUE SERVICE (STARS)
RACCOON CITY, MO

JUNE 1998

PREPARED BY:

UMBRELLA CORPORATION'S SPENCER SECURITY DIVISION
SSH[ghost]
ARKLAY RD, USA 65807

EXECUTIVE SUMMARY

Raccoon City Police Department, also known as RPD, Special Tactics and Rescue Service, also known as STARS, division is an elite special forces division of the Arklay Mountains. The purpose of STARS is to combat increasing terrorism and violent crimes found in Raccoon City and is greatly funded by the private defense contractor Umbrella Corporation. In some cases, STARS may act more like private security for Umbrella Corps interests than public service when applicable. STARS consists of two teams, six members on each team. The purpose of STARS is to act as a local elite forces team for Raccoon City as well as a rescue service for the mountain area outside the city as well. STARS fights urban violence, terrorism, provides RPD and/or Umbrella Corp as needed when needed, and assists in dangerous rescue missions.

RPD STARS contacted Spencer Security as of 6 March 1998 to conduct an assessment and evaluation on computer systems and networks owned and administrated by RPD STARS. The assessment and evaluation lasted from 9 March to 6 June 1998. The assessment is not an inspection, certification, or risk analysis. The purpose of the assessment was to assess the security posture of RPD STARS' computer systems and networks in conjunction with industry standards. The methodology used for the assessment involved the 18 baseline INFOSEC categories and posture analysis, system demonstrations, interviews, and documentation review and the evaluation involved internal and external scanning, network mapping, and assessing technical strengths and weaknesses from scan results. The implementation of any recommendations from Spencer Security is strictly voluntary and at the discretion of RPD STARS' management. The implantation of any recommendations contained herein does not guarantee the elimination of all risks.

The systems assessed were the 911 / Communications system + back-up, communications network, workstation network, database network, and all databases including payroll with server, schedule with server, arrest records, financial records, evidence, employee records, and equipment records. All information of these systems are sensitive, but employee records, evidence, and incident reports are the most sensitive.

The biggest issues revolved around a damaged, critical back-up system, open database network, lack of authorization, and privilege escalation. The back-up system should be repaired and made sure a safe distance away from the live system. The open database should be closed and secure. There should be implementation of an authorization system and logs of privilege escalation. The live communications system was very secure, the use of multiple firewalls diminished success of external attacks, the IDPS system works perfectly fine.

The INFOSEC Posture Rating is a 6.39. The SVCM, OVCM, and IPR can be found in APPENDICES C, D, and E.

We at Spencer Security would like to that the STARS teams for their assistance. We would like to give special thanks to Alpha Team Leader Albert Wesker, Alpha Team IT Specialist Brad Vickers, Bravo Team Leader Enrico Marini, and Bravo Team Communications Specialist

Richard Aiken. Should any of RPD or STARS require further questions in regards to the assistance provided, feel free to contact Wesker at (911) 966 – 2437 ext. 9375, Vickers at (911) 966 – 2437 ext. 8427, Marini at (911) 966 – 2437 ext. 6274, and Aiken at (911) 966 – 2437 ext. 2456.

TABLE of CONTENTS

INTRODUCTION

Raccoon City Police Department, also known as RPD, Special Tactics and Rescue Service, also known as STARS, division is an elite special forces division of the Arklay Mountains. The purpose of STARS is to combat increasing terrorism and violent crimes found in Raccoon City and is greatly funded by the private defense contractor Umbrella Corporation. In some cases, STARS may act more like private security for Umbrella Corps interests than public service when applicable. STARS consists of two teams, six members on each team. The purpose of STARS is to act as a local elite forces team for Raccoon City as well as a rescue service for the mountain area outside the city as well. STARS fights urban violence, terrorism, provides RPD and/or Umbrella Corp as needed when needed, and assists in dangerous rescue missions.

RPD STARS contacted Spencer Security as of 6 March 1998 to conduct an assessment and evaluation on computer systems and networks owned and administrated by RPD STARS. The assessment and evaluation lasted from 9 March to 6 June 1998. The assessment is not an inspection, certification, or risk analysis. The purpose of the assessment was to assess the security posture of RPD STARS' computer systems and networks in conjunction with industry standards. The methodology used for the assessment involved the 18 baseline INFOSEC categories and posture analysis, system demonstrations, interviews, and documentation review and the evaluation involved internal and external scanning, network mapping, and assessing technical strengths and weaknesses from scan results. The implementation of any recommendations from Spencer Security is strictly voluntary and at the discretion of RPD STARS' management. The implantation of any recommendations contained herein does not guarantee the elimination of all risks.

The live communications system was very secure, the use of multiple firewalls diminished success of external attacks, the IDPS system works perfectly fine.

SYSTEM DESCRIPTIONS

The organizational aspects assessed are the equipment records, employee records, incident reports, evidence, financial records, and arrest records including respective databases. The equipment records database is used to store equipment records, employee records database is used to store employee records and background searches, incident reports database is used to store incident reports filed by citizens and police as well as 911 calls, evidence database is used to catalog evidence for digital access but not physical, financial records database is used to store financial records from budgets to income, and arrest records database stores arrest records. Incident reports SQL database is configured with the 911 / Communications system network and the other SQL databases mentioned are configured on their own network.

The systems aspects assessed are communications, IT, emergency, schedule with database, and payroll with database. The 911 / Communications system is configured on its own network to receive calls from outside the building (eg citizens with emergencies) with two serves with

redundancy in case of failure and the incident reports SQL database. The IT system is the entire network and systems infrastructure within STARS, which includes an IDPS and workstation network in addition to the 911 / Communications network and systems and the database network. The emergency system is a physical system with fire alarms, smoke detectors, fire extinguishers, fire escape maps, etc. The schedule and payroll servers are part of the database network complete with own databases.

IMPACT ATTRIBUTE DEFINITIONS

- Confidentiality – No unauthorized access or reading of sensitive internal documents not public information
- Integrity – All records and documents have not been modified without timestamps and digital signatures including team leaders
- Availability – All records and documents are readily accessible to team members / leaders when needed
- Non-repudiation – Team member / leader accountability for actions conducted whether properly or not; eg digital signatures with digital files

IMPACT VALUE DEFINITIONS

High

1. Loss of life / injury
2. System lock-up (no STARS emergency services for 10+ minutes)
3. Increased crime (150%+ in one week)
4. Full loss of evidence / records
5. Loss of funding ($1,000,000 - $78,000,000 (full annual budget))

Medium

1. System lock-up (no STARS emergency services for 1 – 10 minutes)
2. System congestion (emergency services slowed 50%+)
3. Partial loss of evidence / records
4. Loss of funding ($1 - $1,000,000)

Low

1. System lock-up (no STARS emergency service for 0 – 60 seconds)
2. Public embarrassment
3. Slight inconvenience (ie more dash / body cams required)

ORGANIZATIONAL

Critical Information Types

1. Equipment records

2. Employee records / Background searches
3. Incident reports
4. Evidence
5. Arrest records
6. Funding / accounting

Critical Impact Matrix

Information	Confidentiality	Integrity	Availability	Non-Repudiation
Equipment Records	Medium	High	Medium	Medium
Employee Records	High	High	High	Medium
Incident Reports	High	High	High	Medium
Evidence	High	High	High	High
Financial Records	Low	Medium	High	Medium
Arrest Records	Low	High	High	High

Confidentiality is medium for equipment records since leaks can be a loss of records, but new APVs, LPRs, or IMSI catchers won't lead to increased crime in response and thus loss of life or even lock-up. Employee records is high since leaks can lead to a loss of life in case criminals find out law enforcement family members, home address, or undercover identities. Incident reports and evidence are also high since information such as who made a 911 call or what evidence was voluntarily given to law enforcement regarding a criminal's behavior can put that individual in danger. Financial and arrest records are low since both are public information, or supposed to be, already.

Integrity is high for equipment records and employee records which can lead to a loss of life from missing gear and mentally ill officers with a history of violence. Evidence and arrest records can lead to loss of life if suspect released due to tampered evidence or arrest record, thus are also high. Incident reports can lead to a lock-up of emergency services due to fraudulent reports that detract away from actual emergencies, thus can lead to loss of life as well, which makes it high. Financial records are medium since altered records would lead to a loss of funding, but wouldn't lead to a lock-up of emergency services, loss of life, or increased crime.

Availability for equipment records is a medium since a lack of availability won't lead to loss of life nor would it just be a slight inconvenience. Employee records is high for the previously mentioned reason in integrity with officers not being fit for duty. Incident reports, evidence, and arrest records are high for the potential increase in crime and/or loss of life from not having records on certain individuals, incidents, and evidence when needed immediately. Financial records are high / medium due to a potential loss of funding not having financial records when needed, but won't immediately lead to loss of

life, increased crime, or lock-up. However, the amount that could be lost cannot be ascertained so the highest impact value applicable was chosen.

Non-repudiation is a medium for potential records loss with knowing who is accountable, excluding two. Evidence and arrests records can lead to increased crime due to some accountable individuals being found corrupt and tampering with evidence, thus are high.

SYSTEM

Critical Information Types

1. Communications
2. IT
3. Emergency
4. Schedule
5. Payroll

Critical Impact Matrix

System	Confidentiality	Integrity	Availability	Non-repudiation
Communications	High	High	High	High
IT	High	High	High	High
Emergency	High	High	High	High
Schedule	Low	Low	Low	Low
Payroll	Low	High	Low	Medium

Confidentiality is high for communications (911 services), IT, and emergency response (ie fire alarms for precinct) since information about any service becoming public makes tampering easy and can lead to potential loss of life in communications or emergency response or lock-up in communications again or IT. Schedule and payroll are low due to slight inconvenience of adjustments or potential embarrassment of payroll leak.

Integrity is high for communications since failure in communications can lead to increased crime, loss of life, and lock-up. Failure in IT can lead to lock-up and increased crime due to availability being dependent on IT, thus also high. Failure in emergency response such as a fire can lead to loss of life if an aspect such as an alarm and sprinkler system fail to activate, thus also high. I put schedule at low again for inconvenience to change back or create anew. Payroll is at a high since officers that can't be paid are officers that cannot work.

Availability for communications is high since emergency services such as law enforcement are meant to be readily accessible to everyone in need when in need. IT is high since I presume the modern police departments use IT and may have difficulty it

functioning without IT which can lead to lock-up. Emergency response is high since no fire alarms to pull in case of fire means the entire building isn't warned about potential fire, which would lead to a loss of life. Schedule and payroll are low since a lack of availability to either systems are inconvenient at best. **Non-repudiation** is high for communications, IT, and emergency services for previously mentioned reasons. Without accountability when such services fail, we cannot trace back to the origin of the failure in a timely-enough manner. Schedule is low since who creates the schedule isn't all that important since a scheduling system is unlikely to be a high-risk issue. However, who assigns the funds to whom does matter, but would be a loss of funding or records at worst without accountability. Therefore, payroll is medium.

SYSTEM CONFIGURATION

The configuration (see APPENDIX A) shows the telephone system acting through the Internet, but is meant to show when a call is received how it's picked up by 911 services and sent over network in order to record and log calls. In case the primary 911 system fails, there's a back-up and they both save incident reports to respective database. The other servers, databases, and workstations are internal, thus go through another router and firewall, but the workstations are on a different network from the databases and servers. There's also an intrusion detection and prevention system on the internal network.

There are six HP workstations per team, due to alternating shifts, each with HP-UX (UNIX) and Elm 2.4 UNIX mail clients. There are a total of twelve members, thus twelve active accounts and users. Networking services include TCP/IP, POP3, and SMTP for all users. Networking services include TELNET, FTP, and SSH for root users. Routers, switches, and firewalls are all of Cicso brand. There are also four DG/UX (UNIX) servers (two 911 / Communications, one schedule, and one payroll) and a HP LaserJet printer.

The network consists of two routers, two switches, and three firewalls to separate internal networks from outside threats and internal without the proper authorization from root users. One router is set to receive Internet access, which is shielded by the first firewall. The firewall connects to the first switch that connects the 911 / Communications System network to the outside world as well as the second router for the internal network. The 911 / Communications network consists of two 911 / Communication servers in redundancy which connects to the incident reports database. The aforementioned second router connects to the IDPS, firewall for the workstation network, and firewall for the database network. The database network firewall connects to the second switch that connects to the databases equipment records, employee records, evidence, financial records, and arrest records. It also connects to the payroll and schedule servers that connect to their respective databases as outlined in APPENDIX A.

INFOSEC ANALYSIS

HIGH FINDINGS

Finding 01

Title: No Authorization on Database Network
Rating: High
CVE: N/A
CVSS: N/A
Description: Employee records have been found modified without digital signatures. Database network open with no identity verification or authorization system. Permits all users as if with escalated privileges and internal and/or external users access to commit malicious behavior. Destroys record integrity.
Recommendation:

1. Install authorization system with timestamps for attempted access.
2. Limit non-root users access and privileges.
3. Require team leader authorization to access.
4. Monitor root users access.
5. Block external access.

Finding 03

Title: Damaged Back-up 911 / Communications System
Rating: High
CVE: N/A
CVSS: N/A
Description: Back-up 911 / Communications System physically damaged; seemingly electrical. May have been caused by electrical storm or surge overwhelming stielding, may have been faulty, or tampered with by killer USB attack. Experienced spike in voltage and caught fire. Capable of working with replaced parts.
Recommendation:

1. Replaces parts destroyed by surge / fire.
2. Shield server from power surges.
3. Keep safe distance from live system. Keeps both systems from dying at once.
4. Purchase / install CCTV system internally / externally in case of deliberate attack.

MEDIUM FINDINGS

Finding 04

Title: Incident Report Database Glitch
Rating: Medium
CVE: N/A
CVSS: N/A
Description: Several incoming 911 calls from various numbers at random times and locations report feral animal attacks in the Arklay Mountains with rotting flesh. Possible causes are orchestrated prank by local high school students, system breach or modification without authorization (IDPS hasn't picked up anything), or locals have seen actual undying monsters.
Recommendation:

1. Review IDPS logs and confirm working without error.
2. Confirm external access blocked completely.
3. Block non-root access from internal users.
4. Install timestamp system for attempted access.

Finding 06

Title: Remote command execution is DG/UX finger daemon
Rating: Medium
CVE: CVE-1999-0152
CVSS: 7.5
Description: This is a daemon vulnerability in DG/UX servers. The vulnerability exists with the finger daemon allowing remote command execution through shell metacharacters, which means any internal and/or external party can misuse finger for functions not intended to be applicable with fingerd. It partially affects **confidentiality** with information disclosure, **integrity** with limited modification capabilities, and **availability** with some resources being used up by the user exploiting the vulnerability. (www.cvedetails.com/cve/CVE-1999-0152/)
Recommendation:

1. If fingerd isn't essential, disable or remove.
2. If fingerd is essential, remove permissions and access from non-root personnel. Update policy on the use of root scripts, daemons, and programs.

Finding 08

Title: Restriction bypass in HP Laserjet printers
Rating: Medium
CVE: CVE-1999-1062
CVSS: 7.5
Description: This is a printer vulnerability in HP Laserjet printers with JetDirect cards. The vulnerability exists when connected to a network with TCP/IP configured allowing an internal and/or external party to issue remote command execution that bypasses print filters to TCP ports 9099 and 9100 using PostScript documents. It partially affects **confidentiality** with information disclosure, **integrity** with limited modification capabilities, and **availability** with some resources being used up by the user exploiting the vulnerability.
(www.cvedetails.com/cve/CVE-1999-1062/)
Recommendation:

1. If printing from a network isn't essential, disable or remove networking capability.
2. Configure network settings to only be accessible internally and change TCP ports away from default.
3. Replace printers with alternative.

LOW FINDINGS

Finding 02

Title: Suspicious Outbound Network Traffic
Rating: Low
CVE: N/A
CVSS: N/A
Description: Constant email traffic found inbound and outbound to and from Umbrella Corporation. Firewall rules are not set to include or exclude email communication with local businesses through whitelisting or blacklisting. While not necessarily an issue, it is abnormal. May be a breach, but IDPS shows no signs of malicious behavior from email traffic.
Recommendation:

1. Adjust firewall rules to limit external email traffic size and frequency.
2. Update email policy to deter external email use.
3. Create schedule reviews of IDPS for any and all traffic.

Finding 05

Title: Privilege escalation in HP-UX
Rating: Low
CVE: CVE-1999-1311
CVSS: 4.6
Description: This is a workstation vulnerability in the Hewlett-Packard PCs with HP-UX 10.10 and 10.20 operating systems installed. The vulnerability exists within dtlogin and dtsession allowing local users to bypass authentication and gain root privileges, which means any STARS member can have the same level of privilege as the Alpha and Bravo team leaders. It partially affects **confidentiality** with information disclosure, **integrity** with limited modification capabilities, and **availability** with some resources being used up by the user exploiting the vulnerability. (www.cvedetails.com/cve/CVE-1999-1311/)
Recommendation: Update HP-UX variants to HP-UX 10.24, 10.30, or 11.00. 10.24 is a compartmentalized operating system and may not fit the needs and fluid update without production decrease like with 10.30 or 11.00.

Finding 07

Title: Remote command execution in Elm
Rating: Low
CVE: CVE-1999-0114
CVSS: 4.6
Description: This is a mail client vulnerability in Elm 2.4 UNIX mail client. The vulnerability exists within the filter utility where any STARS member can delete a temporary file and create a symlink to the victim's mail spool in order to retrieve said victims email messages. It partially affects **confidentiality** with information disclosure, **integrity** with limited modification capabilities, and **availability** with some resources being used up by the user exploiting the vulnerability. (www.cvedetails.com/cve/CVE-1999-0114/)
Recommendation:

1. Update UNIX mail client elm 2.4 to elm 2.4.25.
2. Restrict the amount of temporary files that can be created and limit symlink usage to root users only.
3. Replace UNIX mail client with alternative

CONCLUSION

An INFOSEC Posture Rating of 6.39 is close to the median. However, this doesn't mean STARS is safe with the current security posture. The goal is to get as close to 3 as possible and to stay away from 9. The biggest issues revolved around a damaged, critical back-up system, open database network, lack of authorization, and privilege escalation. The back-up system should be repaired and made sure a safe distance away from the live system. The open database should be closed and secure. There should be implementation of an authorization system and logs of privilege escalation. The best means to fix these vulnerabilities are to implement the recommendations found in INFOSEC Analysis.

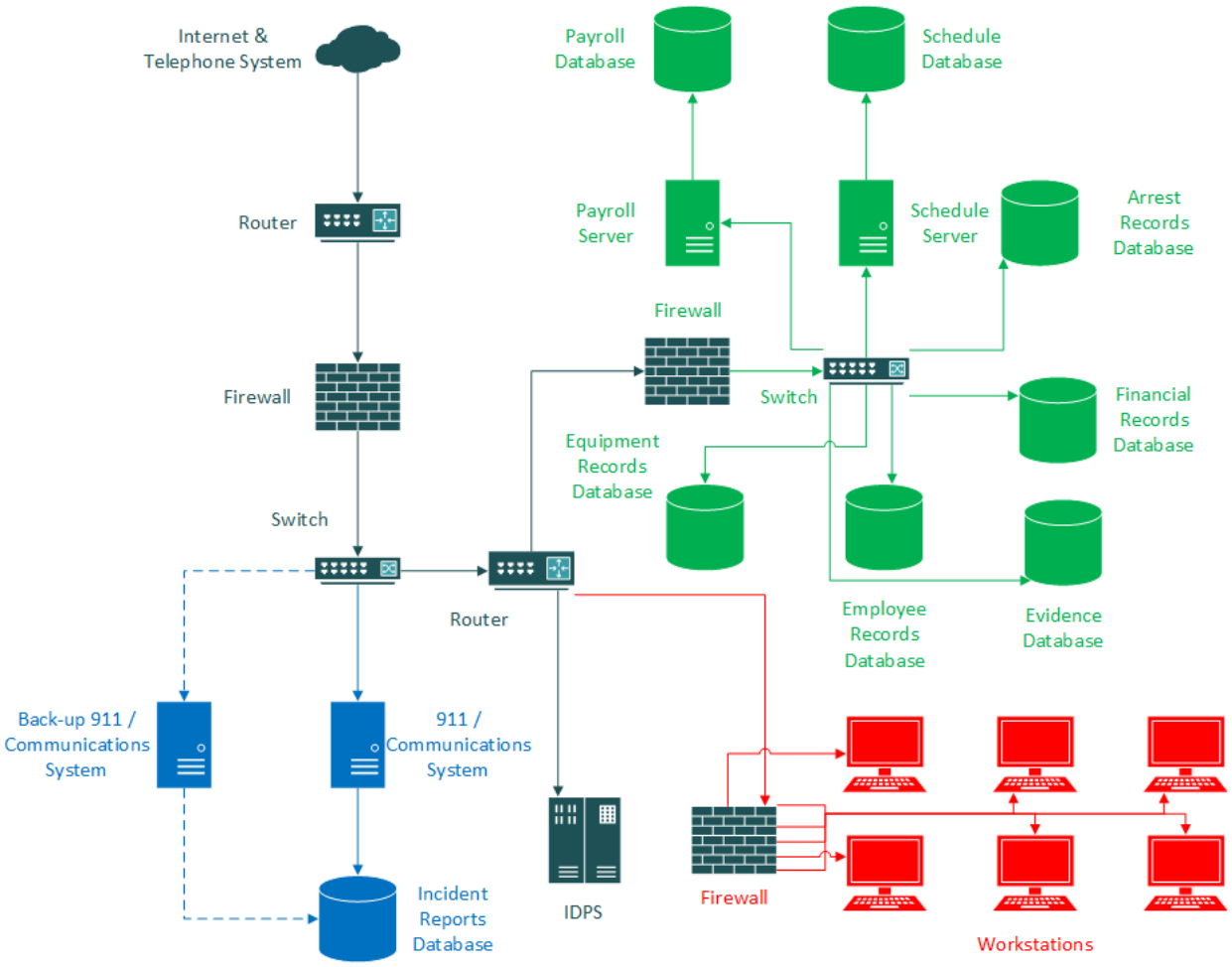
While security implementation or even assessments and evaluation are costly, security exploitation and/or failure is even greater. While the assessment and evaluation standalone or together did not cost the RPD STARS full annual budget of $78,000,000, a critical security failure that could have been avoided could cost the entire full annual budget. It's better to be safe than sorry.

Spencer Security's recommendations are suggested guidelines and not requirements in order to assist RPD STARS improve their current security posture. Implementation of any of the recommendations should be done at the discretion of the STARS team leads.

Should any of RPD or STARS require further questions in regards to the assistance provided, feel free to contact Wesker at (911) 966 – 2437 ext. 9375, Vickers at (911) 966 – 2437 ext. 8427, Marini at (911) 966 – 2437 ext. 6274, and Aiken at (911) 966 – 2437 ext. 2456.

APPENDICES

APPENDIX A – Network Diagram



APPENDIX B – Technical Evaluation Plan

Raccoon City Police Department – STARS (Special Tactics & Rescue Service)

Contact Information

Wesker, Albert
RPD STARS Division Leader / Alpha Team Leader
Email: a.wesker@rpd.org
Phone: (911) 966 – 2437 ext. 9375

Marini, Enrico
RPD STARS Bravo Team Leader
Email: e.marini@rpd.org
Phone: (911) 966 – 2437 ext. 6274

Mission

The RPD STARS division is an elite special forces division of the Arklay Mountains. Ex-military personnel and exceptionally academic civilians on par with national defense or STEM (Science, Technology, Engineering, Math) work are preferred. The purpose of STARS is to combat increasing terrorism and violent crimes found in Raccoon City and is greatly funded by the private defense contractor Umbrella Corporation. In some cases, STARS may act more like private security for Umbrella Corps interests than public service when applicable.

The purpose of STARS is to act as a local elite forces team for Raccoon City as well as a rescue service for the mountain area outside the city as well. STARS fights urban violence, terrorism, provides RPD and/or Umbrella Corp as needed when needed, and assists in dangerous rescue missions.

Methodology Overview

The INFOSEC Evaluation Methodology, or IEM, is the hands-on aspect for evaluating a customers' network and system using technical evaluation tools in an effort to find potential vulnerabilities. The IEM is not a Red Team effort, thus consists of no penetration testing. In other words, the IEM is meant to find vulnerabilities, report them, and detail recommendations, but the IEM is not meant to exploit said vulnerabilities for any reason whatsoever. The IEM is a part of the NSA toolkit in order to conduct security reviews of the customer and was created with use within the private sector in mind. The benefits of the IEM are that it finds technical vulnerabilities already existing within the customers' network and/or systems and recommends patches or security fixes to said vulnerabilities, but the level of detail for the vulnerabilities and recommendations is up to the customer to decide. The results will be a scan as detailed and thorough as per customer compliance complete with proper adjustments in mind. The final report will detail the customers' technical security in sections broken down to allow for

comprehension and implementation of recommendations. The 10 IEM baseline activities, with tools, to be conducted for technical information collection of the current security posture are as follows:

- **Port Scanning**
  1. Network Mapper (Nmap) v7 https://nmap.org/
  2. WUPS v1.4 ntsecurity.nu/toolbox/wups/
- **SNMP Scanning**
  1. SNScan v1.05 www.mcafee.com/us/downloads/free-tools/snscan.aspx
- **Enumeration / Banner Grabbing**
  1. Netcat v1.10 nc110.sourcefourge.net
  2. Network Mapper (Nmap) v7 https://nmap.org/
- **Wireless Enumeration**
  1. NetStumbler v0.40 www.netstumbler.com
  2. Kismet v2013-03-R1b https://kismetwireless.net
- **Vulnerability Scanning**
  1. Nexpose – Community Edition www.rapid7.com/products/nexpose/
  2. OpenVAS v8 www.openvas.org
- **Host Evaluation**
  1. MS Baseline Security Analyzer v2.3 www.microsoft.com/en-us/download/details.aspx?id=7558
- **Network Device Analysis**
  1. Network Device Analyzer (NDASoft) v1.0.1 network-device-analyzer.soft112.com
- **Password Compliance Testing**
  1. RainbowCrack v1.6.1 http://project-rainbowcrack.com/
  2. HashCat v2.01 http://hashcat.net/oclhashcat/
  3. Medusa v2.2 http://foofus.net/goons/jmk/medusa/medusa.html
  4. OphCrack v3.6 http://ophcrack.sourceforge.net/
- **Application-Specific Training**
  1. Ike-Scan v1.9 http://www.nta-monitor.com/tools-resources/security-tools/ike-scan
- **Network Sniffing**
  1. Netsniff-ng v0.6.0 https://github.com/netsniff-ng/netsniff-ng/releases
  2. Wireshark v 1.10.6 https://www.wireshark.org/

Organizational Information Criticality

Critical Organizational Information

1. Equipment records
2. Employee records / Background searches
3. Incident reports
4. Evidence
5. Arrest records
6. Funding / accounting

Impact Attributes

- Confidentiality – privacy / records security
- Integrity – unmodified / original records (edits from authorized personnel with non-repudiation)
- Availability – records access / organized system / neat accounting
- Non-repudiation – authorized personnel actions on records / accountability to actions

Critical Impact Value Definitions

High

1. Loss of life / injury
2. System lock-up (no emergency services)
3. Increased crime
4. Full loss of evidence / records
5. Loss of funding ($1,000,000 - $78,000,000 (full annual budget))

Medium

1. System congestion (emergency services slowed)
2. Partial loss of evidence / records
3. Loss of funding ($1 - $1,000,000)

Low

1. Public embarrassment
2. Slight inconvenience (ie more dash / body cams required)

Organizational Information Criticality Matrix

Information	Confidentiality	Integrity	Availability	Non-Repudiation
Equipment Records	Medium	High	Medium	Medium
Employee Records	High	High	High	Medium
Incident Reports	High	High	High	Medium
Evidence	High	High	High	High
Financial Records	Low	Medium	High	Medium
Arrest Records	Low	High	High	High

Confidentiality is medium for equipment records since leaks can be a loss of records, but new APVs, LPRs, or IMSI catchers won't lead to increased crime in response and thus loss of life or even lock-up. Employee records is high since leaks can lead to a loss

of life in case criminals find out law enforcement family members, home address, or undercover identities. Incident reports and evidence are also high since information such as who made a 911 call or what evidence was voluntarily given to law enforcement regarding a criminal's behavior can put that individual in danger. Financial and arrest records are low since both are public information, or supposed to be, already.

Integrity is high for equipment records and employee records which can lead to a loss of life from missing gear and mentally ill officers with a history of violence. Evidence and arrest records can lead to loss of life if suspect released due to tampered evidence or arrest record, thus are also high. Incident reports can lead to a lock-up of emergency services due to fraudulent reports that detract away from actual emergencies, thus can lead to loss of life as well, which makes it high. Financial records are medium since altered records would lead to a loss of funding, but wouldn't lead to a lock-up of emergency services, loss of life, or increased crime.

Availability for equipment records is a medium since a lack of availability won't lead to loss of life nor would it just be a slight inconvenience. Employee records is high for the previously mentioned reason in integrity with officers not being fit for duty. Incident reports, evidence, and arrest records are high for the potential increase in crime and/or loss of life from not having records on certain individuals, incidents, and evidence when needed immediately. Financial records are high / medium due to a potential loss of funding not having financial records when needed, but won't immediately lead to loss of life, increased crime, or lock-up. However, the amount that could be lost cannot be ascertained so the highest impact value applicable was chosen.

Non-repudiation is a medium for potential records loss with knowing who is accountable, excluding two. Evidence and arrests records can lead to increased crime due to some accountable individuals being found corrupt and tampering with evidence, thus are high.

System Information Criticality

Critical System Information

1. Communications
2. IT
3. Emergency
4. Schedule
5. Payroll

Impact Attributes

- Confidentiality – privacy / records security

- Integrity – unmodified / original records (edits from authorized personnel with non-repudiation)
- Availability – records access / organized system / neat accounting
- Non-repudiation – authorized personnel actions on records / accountability to actions

Critical Impact Value Definitions

High

1. Loss of life / injury
2. System lock-up (no emergency services)
3. Increased crime
4. Full loss of evidence / records
5. Loss of funding ($15,000,000 - $78,000,000 (full annual budget))

Medium

1. System congestion (emergency services slowed)
2. Partial loss of evidence / records
3. Loss of funding ($1,000,000 - $15,000,000)

Low

1. Public embarrassment
2. Slight inconvenience (ie more dash / body cams required)
3. Loss of funding ($1 - $1,000,000)

System Informational Criticality Matrix

System	Confidentiality	Integrity	Availability	Non-repudiation
Communications	High	High	High	High
IT	High	High	High	High
Emergency	High	High	High	High
Schedule	Low	Low	Low	Low
Payroll	Low	High	Low	Medium

Confidentiality is high for communications (911 services), IT, and emergency response (ie fire alarms for precinct) since information about any service becoming public makes tampering easy and can lead to potential loss of life in communications or emergency response or lock-up in communications again or IT. Schedule and payroll are low due to slight inconvenience of adjustments or potential embarrassment of payroll leak.

Integrity is high for communications since failure in communications can lead to increased crime, loss of life, and lock-up. Failure in IT can lead to lock-up and increased crime due to availability being dependent on IT, thus also high. Failure in emergency response such as a fire can lead to loss of life if an aspect such as an alarm and

sprinkler system fail to activate, thus also high. I put schedule at low again for inconvenience to change back or create anew. Payroll is at a high since officers that can't be paid are officers that cannot work.

Availability for communications is high since emergency services such as law enforcement are meant to be readily accessible to everyone in need when in need. IT is high since I presume the modern police departments use IT and may have difficulty it functioning without IT which can lead to lock-up. Emergency response is high since no fire alarms to pull in case of fire means the entire building isn't warned about potential fire, which would lead to a loss of life. Schedule and payroll are low since a lack of availability to either systems are inconvenient at best.

Non-repudiation is high for communications, IT, and emergency services for previously mentioned reasons. Without accountability when such services fail, we cannot trace back to the origin of the failure in a timely-enough manner. Schedule is low since who creates the schedule isn't all that important since a scheduling system is unlikely to be a high-risk issue. However, who assigns the funds to whom does matter, but would be a loss of funding or records at worst without accountability. Therefore, payroll is medium.

Customer Concerns

1. Do we still have a line of support to 911 calls if own dispatch system has fallen? (STARS dispatch system, not RPD since operating in specific sect within RPD HQ.)
2. Are the maintenance and critical-for-survival guides up-to-date with accurate information?
3. Do we test our own systems thoroughly enough or as frequently as needed?
4. Can one team still encompass mission goals if the other has fallen?
5. Are our system logs of critical information or even critical information secure enough from outside threats? How necessary is non-repudiation from potential internal incidents?
6. Are schedule and payroll systems secure internally and externally?
7. Do the Incident Reports and Beyond Purpose Reports (ie Assisting RPD and/or Umbrella beyond urban violence, terrorism, or rescue purposes) regarding Umbrella Corp. need to be reviewed?
8. How long can we function BAU during a building-wide blackout?
9. Are our shifts separate enough or do we need to create a third shift for load-balancing purposes in case one team falls? If yes, should we recruit more former military personnel and/or extraordinary civilians or should we shift the teammates roles in our current teams?
10. Should all of our officers wear bodycams? If yes, what is our most realistic approach to increased data storage of recorded footage?
11. Can scanning against our 911 / communication systems knock it offline?
12. Will our IDPS still pick up IEM traffic during scan?

13. Are the network devices and 3 networks scanned all at once or can they be done one at a time for compartmentalization and easier detailing?
14. Can the IEM team conduct scans against the network devices and 2 of the networks on the same shift as Alpha Team, excluding the 911 / communications network, so Brad Vickers, our IT specialist, can assist in bringing the network and systems back online in case of a network failure? Can the IEM team conduct scans against the 911 / communications network during Bravo Team's shift so that Richard Aiken, our communications specialist, can do the same in case of a similar incident?

Customer Constraints

- 911 / Communications System cannot go offline. Each system must be scanned individually of each other in case of system failure.
- Communications Specialist Richard Aiken and IT Specialist Brad Vickers work on alternating shifts. Network devices, workstation network, and database network must be scanned during Brad Vickers' shift and 911 / communications system network must be scanned on Richard Aiken's shift.
- STARS operates as public, emergency service, thus needs to operate 24/7 without fail. Network cannot crash.
- Evaluation team cannot conduct scans without team lead being immediately accessible respective to current shift.
- Ignore any findings on systems regarding monstrous creatures, undead individuals, or citizens that have gone missing in the Arklay Mountains.
- Can't use Metasploit (previous IEM consultant team used exploiting tools for vulnerability scanning).

System Configuration / Detailed Network Information

The configuration shows the telephone system acting through the Internet, but is meant to show when a call is received how it's picked up by 911 services and sent over network in order to record and log calls. In case the primary 911 system fails, there's a back-up and they both save incident reports to respective database. The other servers, databases, and workstations are internal, thus go through another router and firewall, but the workstations are on a different network from the databases and servers. There's also an intrusion detection and prevention system on the internal network.

Contact Information

Vickers, Brad **[STARS Network / Workstation Network / Database Network]**
RPD STARS IT Specialist (Alpha Team [Night Shift])
Email: b.vickers@rpd.org
Phone: (911) 966 – 2437 ext. 8427

Aiken, Richard **[911 / Communications System Network]**

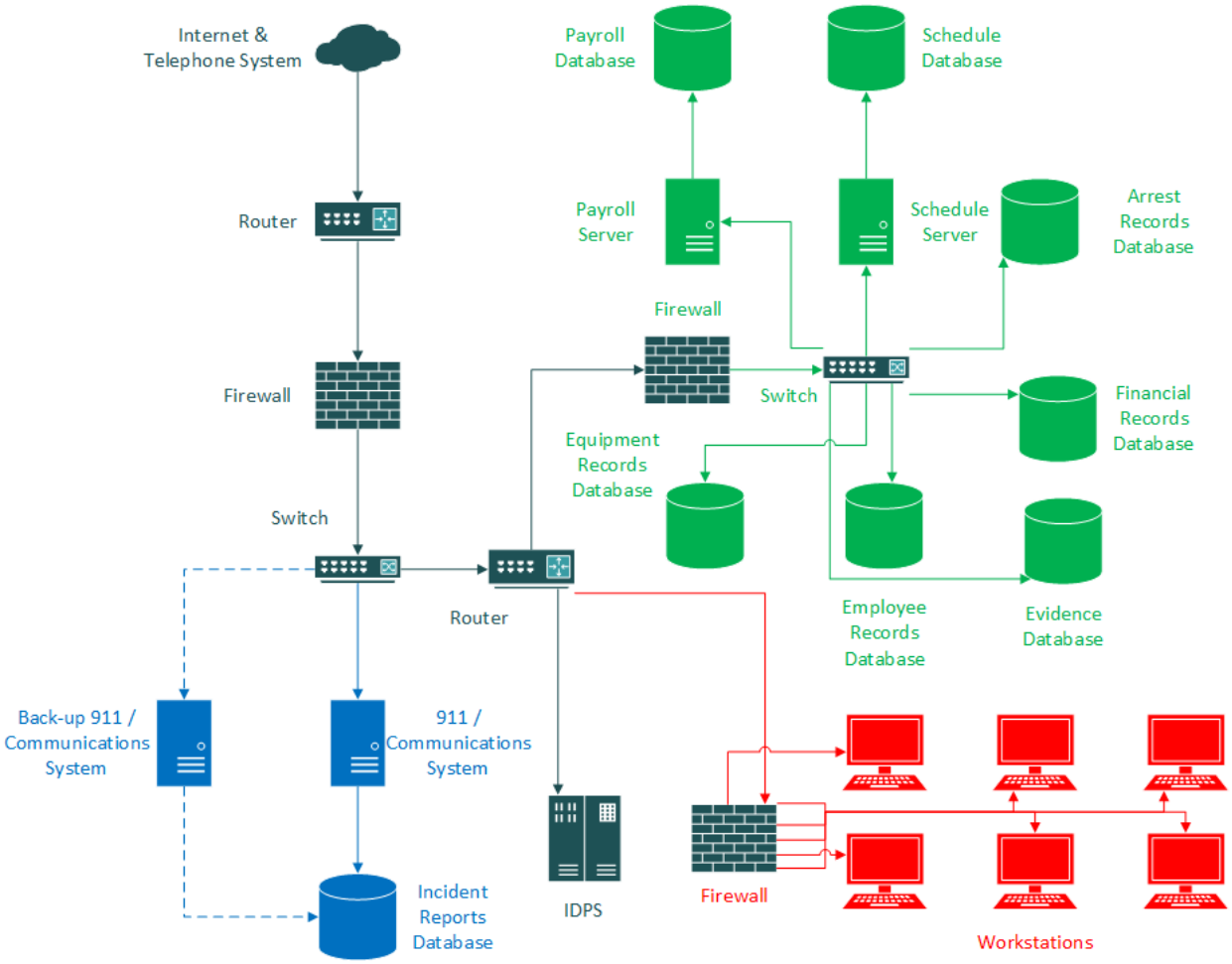
RPD STARS Communications Specialist (Bravo Team [Day Shift])
Email: r.aiken@rpd.org
Phone: (911) 966 – 2437 ext. 2456

Physical Boundaries

Physical workstations and servers permitted access. Physical phone jacks, cables, power sources, doors, locks, and fire alarms permitted access. Customer has allowed testing electronic locks to riot room with combat gear, but has limited access to only the locks and door. Physical access to evidence room and physical copies of non-electronic records / paperwork limited to team leader supervision and requires authorization.

IP Ranges / Subnets

No ranges / subnets specified by customer; gave complete access to entire network. Only restricted what was scanned at what time with what tool. Stated will specify IP addresses only during internal scanning.



Individuals / Positions to be Interviewed

Alpha Team	**Position**	**Formation**
1. Albert Wesker	Division Leader	Team Leader
2. Chris Redfield	Sharpshooter / Co-pilot	Pointman
3. Brad Vickers	Pilot / IT Specialist	Rear Guard
4. Jill Valentine	B&E Specialist	Rear Guard
5. Joseph Frost	Maintenance Supervisor	Floater (rec gear)*
6. Barry Burton	Weapons Supervisor	Support

Bravo Team	**Position**	**Formation**
1. Enrico Marini	Team Leader	Team Leader
2. Kenneth Sullivan	Chemist	Pointman (rec gear)*
3. Rebecca Chambers	Chemical && Medicinal Specialist	Rear Guard
4. Edward Dewey	Pilot	Rear Guard
5. Forest Speyer	Maintenance / Sharpshooter	Floater
6. Richard Aiken	Communications Specialist	Support

Rec gear – reconnaissance gear such as always-recording bodycams

Documents Reviewing

1. RPD Manual
2. Rescue / Survival Guide
3. System Logs
    a. Equipment Records
    b. Employee Records
    c. Incident Reports
    d. Evidence
    e. Finance Records
    f. Arrest Records
4. IDPS Logs
5. Firewall Rules / Logs
6. 911 System
7. Internal Communications Maintenance
8. Network Logs
9. Emergency System Updates
10. Schedule / Payroll Logs
11. Beyond-Purpose Reports (ie Assisting RPD and/or Umbrella beyond urban violence, terrorism, or rescue purposes)
12. Medicinal Herb / Chemical Guide

13. Maintenance Guides
    a. Weapons
    b. Transportation
    c. Communications
    d. Security
    e. Network
    f. Tactical Gear
14. (ALL) Systems Tests Reports

Rules of Engagement

- STARS will provide a long, fold-up table, two chairs, phone access, fax access, printer access, network access, and 911 / Communications System access during internal portion of scan.
- STARS will provide internal static IP addresses during internal scan.
- STARS has agreed on the use of 10.10.220.0/24 during external scan.
- STARS will review any notes and reports created during the IEM to ensure no sensitive information leaves the premises.
- STARS will provide vacant “employee” locker to evaluation team to keep sensitive documents within premises when scans are not being conducted.
- STARS has permitted scanning of STARS network, database network, and workstation network during Alpha Team shift during non-peak hours 03:00 – 7:00
- STARS has permitted scanning of 911 / Communications System network during Bravo Team shift during non-peak hours from 12:00 – 16:00.
- IEM team will notify team lead and team specialist of incident when incident occurs or of immediate vulnerabilities. IEM team will notify team specialists schedule prior to scanning for every scanning.
- STARS has provided Alpha Team Leader Albert Wesker and Alpha Team IT Specialist Brad Vickers contact information and location in case of incident.
- STARS has provided Bravo Team Leader Enrico Marini and Bravo Team Communications Specialist Richard Aiken contact information and location in case of incident.
- STARS has approved the previously mentioned scanning tools, apart from Metasploit, for use and has restricted to simultaneous IP address use to 3 to avoid accidental DoS attack.

Coordination Efforts

STARS has specified ***medium*** level of detail for the executive summary for any STARS personnel to comprehend without abundance of complexity as well as a ***low*** level of detail for the technical report since Vickers and Aiken are able to understand and implement recommendations without needing a medium level of detail.

Deliverables

- Technical Evaluation Plan
- Daily Status Report
- Preliminary Findings
- Immediate Recommendations (potential zero-day vulnerabilities)
- Final Report with Recommendations

Letter of Authorization

The Information Security evaluation is performed under the Agreement of the benefit of the customer, Raccoon City Police Department Special Tactics and Rescue Service division, hereafter referred to as STARS, which gives the evaluation team, Spencer Security, full authority to perform said evaluation.

STARS hereby authorizes Spencer Security to perform an Information Security evaluation on STARS' computer systems and/or networks within the scope of the Agreement.

STARS will not hold Spencer Security liable for any loss of service or data resulting from the Information Security evaluation when conducted within the scope of the Agreement.

STARS shall provide Spencer Security with all necessary information to perform the Information Security evaluation and STARS understands and accepts the risk that said evaluation conducted with the scope of the Agreement may inadvertently cause a server to crash and/or result in loss of service or data.

STARS understands and accepts that Spencer Security makes no representation or warranty that its information security services will prevent system compromise. Spencer Security will provide qualified personnel and perform services consistent with best industry practices.

STARS does further remise, release and discharge Spencer Security, and its respective officers, agents, and employees, from liabilities, obligations, claims, demands and rights of action, including incidental and consequential damages accrued or which may hereafter accrue under or arise from the Information Security evaluation conducted within the scope of the Agreement except to the extent of any negligence, fault, act, or omission of Spencer Security, its employees or agents.

Time-Line of Events
09 March – 06 June 1998

Pre-Assessment
09 March

1. Categorize / Define Information Value
2. Identify Systems & Boundaries
3. Collect System / Security Documents

10 March

1. Generate Assessment Plan

Team Assignment & Coordination

11 – 25 March

(varies from specialists gathered for specific functions from pre-assessment phase)

On-Site Visit

Information Analysis Team

26 – 28 March

1. 18 Baseline INFOSEC Categories / Posture Analysis

29 March – 02 April

1. Document Review

03 – 06 April

1. Interviews

Security Analysis Team

26 – 27 March

1. System Demonstrations

28 March – 06 April

1. Non-intrusive Scans
    a. Internal: 28 March – 03 April
    b. External: 28 March – 03 April
    c. Network mapping: 04 April – 06 April

07 – 08 April

1. Strengths & Weaknesses

Analysis & Report Generation

09 April – 05 June

1. Generate Final Analysis Report

06 June

2. Deliver Final Analysis Report

APPENDIX C – System Vulnerability Criticality Matrix

COMMUNICATIONS NETWORK / SYSTEM

911 / Communications Vulnerability Criticality Matrix	Finding Number	Severity	High	Medium	Low
			Incident Report Confidentiality	Incident Report Integrity	Incident Report Availability
Organizational	3	H	9	7.5	6
Organizational	4	M	7.5	6	4.5
CVE-1999-0152	6	M	7	6	5
Organizational	2	L	6	4.5	3
CVE-1999-0114	7	L	6		

INTERNAL NETWORK (DATABASE + WORKSTATION NETWORKS)

Internal (Database + Workstation) Vulnerability Criticality Matrix	Finding Number	Severity	High										Medium			Low	
			Equipment Records Integrity	Employment Records Confidentiality	Employment Records Integrity	Employment Records Availability	Evidence Confidentiality	Evidence Integrity	Evidence Availability	Financial Records Availability	Arrest Records Integrity	Arrest Records Availability	Equipment Records Confidentiality	Equipment Records Availability	Financial Records Integrity	Financial Records Confidentiality	Arrest Records Confidentiality
Organizational	1	H	9	9	9	9	9	9	9	9	9	9	7.5	7.5	7.5	6	6
CVE-1999-0152	6	M	7	7	7	7	7	7	7	7	7	7	6	6	6	5	5
CVE-1999-1062	8	M	7	7	7	7	7	7	7	7	7	7	6	6	6	5	5
CVE-1999-1311	5	L	5	5	5	5	5	5	5	5	5	5	4	4	4	3	3

APPENDIX D – Organizational Vulnerability Criticality Matrix with Computer Network Defense & INFOSEC Posture Profile

Internal (Database + Workstation) Vulnerability Criticality Matrix INFOSEC Posture Profile Protect = 11 Detect = 1 Respond = 3 Sustain = 0	Finding Number	Computer Network Defense (CND)	Systems Affected	Severity	High											Medium				Low		
					Incident Report Confidentiality	Equipment Records Integrity	Employment Records Confidentiality	Employment Records Integrity	Employment Records Availability	Evidence Confidentiality	Evidence Integrity	Evidence Availability	Financial Records Availability	Arrest Records Integrity	Arrest Records Availability	Incident Report Integrity	Equipment Records Confidentiality	Equipment Records Availability	Financial Records Integrity	Financial Records Confidentiality	Arrest Records Confidentiality	Incident Report Availability
Organizational	1	P	I	H		9	9	9	9	9	9	9	9	9	9		7.5	7.5	7.5	6	6	
Organizational	3	R	C	H	9											7.5						6
Organizational	4	P	C	M	7.5											6						4.5
CVE-1999-0152	6	P	C,I	M		7	7	7	7	7	7	7	7	7	7		6	6	6	5	5	
CVE-1999-1062	8	P	I	M		7	7	7	7	7	7	7	7	7	7		6	6	6	5	5	
Organizational	2	D	C	L	6											4.5						5
CVE-1999-0114	7	P	C	L	6																	3
CVE-1999-1311	5	P	I	L		5	5	5	5	5	5	5	5	5	5		4	4	4	3	3	

APPENDIX E – INFOSEC Posture Rating

HIGH (99) + MEDIUM (337.5) + LOW (30) / TOTAL (73) = 466.5 / 73 = 6.39
IPR = 6.39

06 June 1998
Spencer Security