



IRW INTERNAL SECURITY: INTERIM REPORT

Brief Version Sec&
YUL-816-924I

Study Conducted
by **Sec& – Security System**
for **IRW – Iron Ridge Water**

To Dr. [REDACTED],
&
To whom it should concern.

Having reviewed all of IRW's security systems, we must conclude with a G-level warning. According to our G3 Security Assessment, both systems were rated [REDACTED], based on comparison to industries standards, IRW closest competitors, as well as both IRW' and Sec&' own guidelines.

At the core lies [REDACTED].
That is why we remind you to [REDACTED].
Current conditions constitute a grade-10 threat to [REDACTED]; [REDACTED]
as well as [REDACTED].

For instance, [REDACTED]
Results show that no [REDACTED]
according to every criteria, [REDACTED], as you will see, a serious security
breach.

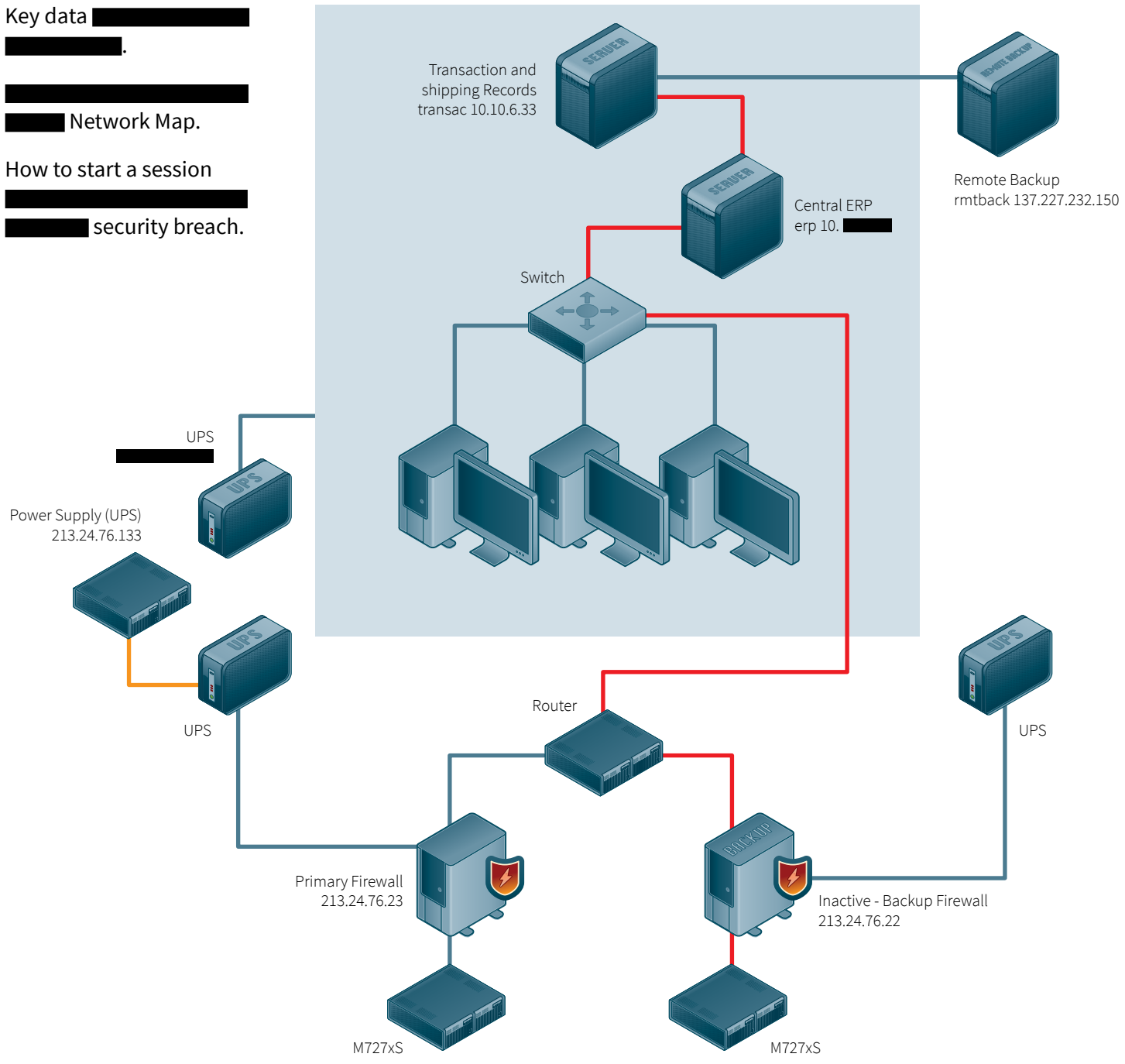
Key is [REDACTED], yet again. [REDACTED]
[REDACTED], such as the **backdoor**, too easily accessible to **control power supply**. [REDACTED]
[REDACTED]. **Power failure** would therefore affect the whole **firewall**, which
in turn might trigger a chain reaction, including **further infiltration** from both outside and
within the company system.

IRW INTERNAL SECURITY: INTERIM REPORT

Key data [REDACTED]
[REDACTED].

[REDACTED]
[REDACTED] Network Map.

How to start a session
[REDACTED]
[REDACTED] security breach.



Simulation of a successful attack

Start your terminal.
Login with any credential.

First, we have to access the vulnerable UPS and shutdown the power to the firewall.

```
VPN 213.24.76.133  
ups shutdown outlet4  
VPN exit
```

This will trigger a failover on the backup firewall. This firewall do not have IP restriction active. This enable someone to enter the internal network. Once there, the attacker can overwrite the backup procedure and trigger a full remote upload of all confidential information in the Transaction and shipping Records.

Example:

```
VPN 213.24.76.22  
setconfig transac remotebackup 0.0.0.0 - (Replace 0.0.0.0 by any compatible external IP)  
remotebackup initiate
```

In sum, to whole system is still far too vulnerable. Immediate measures shall be taken to prevent the system to be either hacked, cracked, or even attacked.

Implement recommendation as previously stated in both our latest report # 765-321 is required.

Safely yours,

Randall Recchi
Security Head
uid rrecchi