



A Layered Approach to Securing Remote Maintenance Consoles

Executive Summary

Availability and security of networks for remote locations are tied directly together. Due to the requirements to keep the network operating at a high level, there needs to be fast access to equipment in case of an outage or problem. People at the operations desk need to be able to connect remotely to telecom equipment such as routers, switches and firewalls or remote servers if users are experiencing troubles. Traditionally administrators have used Telnet to connect to remote devices to configure, troubleshoot or reboot them. In many cases Telnet has been replaced with SSH to take advantage of the encryption capabilities, the thought being that it enhances the security. These services run on the devices at the remote and allow "at the rack" connectivity in most cases. These are referred to as in-band solutions as the traffic that is being used to access the device shares the same path and bandwidth as the user application data traffic.

When you ask network operators how these services work, typically they tell you they work fine. They give excellent connectivity and most operators are extremely familiar with the command line interface of each device to configure or troubleshoot the device. In addition, the cost of these access methods is zero as the services are on almost every networking device and clients are on almost all workstations that are used for access.

While these maintenance interfaces are working fine for network operators and system administrators who are managing the network, they work just as well for those who would like to intrude into the network for malicious intent or just to see what is going on. This paper discusses a layered approach of how to close these interfaces to intruders, make it more difficult for them to find the maintenance interface and keep the authorized management people capable of performing their job better.

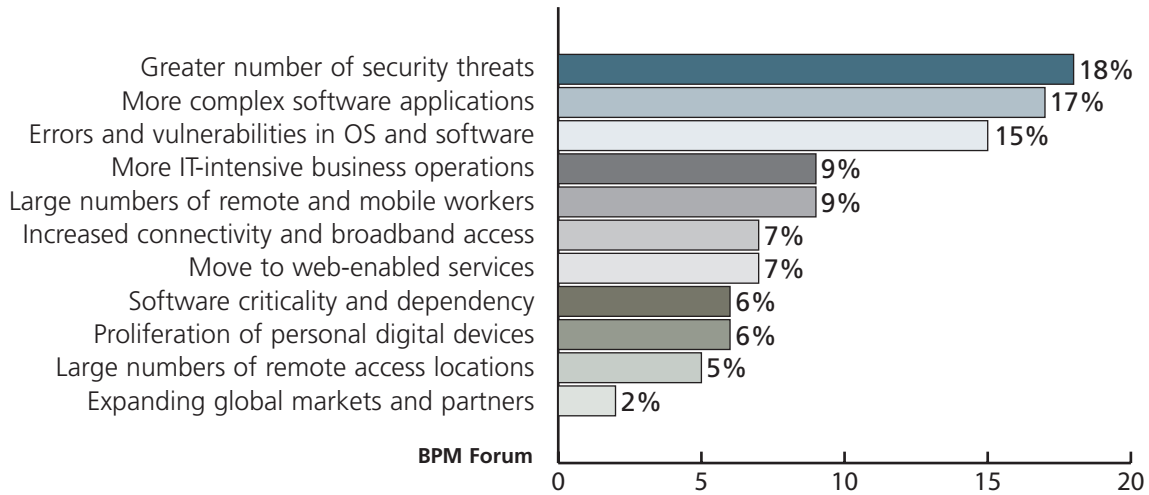
Each year the reliance of companies on their network increases. The network grows in both size and complexity. New applications are added that meet a specific objective oriented towards individual groups. Systems are pushed further and further out into the field where the customer contact resides. Point of sale systems, inventory, receivables collection, human resources and other similar services are no longer restricted to the headquarters location. Pushing these critical applications out into the network means that the availability of the network is critical to smooth business continuation. Along with the applications being pushed further out, data required to support those applications is pushed out as well.

Introduction

Remote office networks continue to abound in today's business environment. Surveys show that by 2010 there will be upwards of 900,000,000 remote workers. Banks and retail have placed systems that support customer touch services to speed up the processing of transactions. Inventory systems have been pushed out into the field along with processing for synergistic offerings that increase the reliance on the network. Companies have strategic relationships with both customers and suppliers that place access to the network on their customers' or suppliers' premises. The complexity of the networks and the applications needed to support the business and maintain the competitive edge grows with every new service rollout.

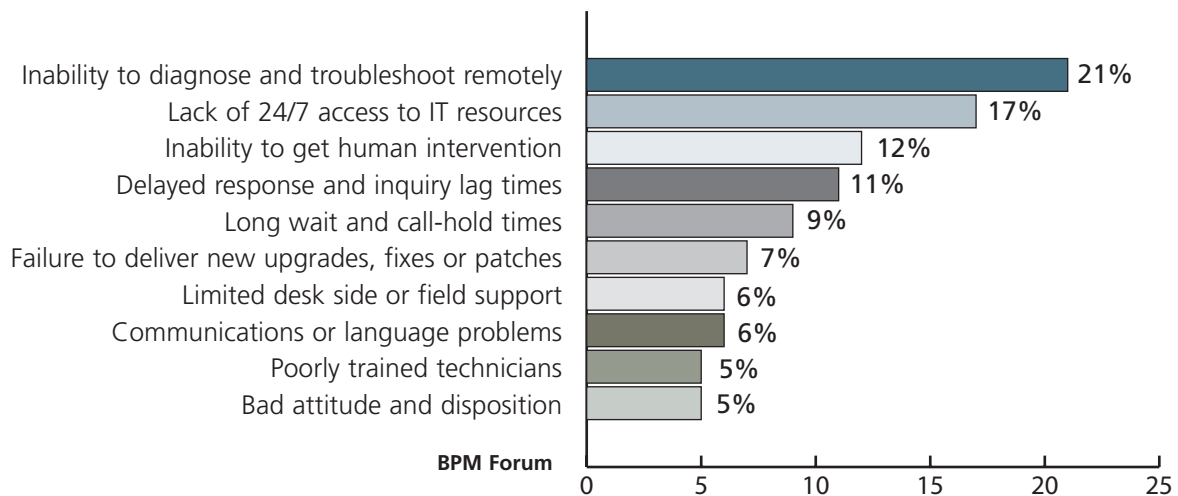
Executives charged with the responsibility to operate corporate networks face an ever increasing challenge. A survey conducted by the Business Performance Management Forum of 400+ senior executives spread across a wide spectrum of businesses, shows what concerns this increased complexity is causing within their ranks.

Question: What is the most important factor multiplying IT operational support demands?



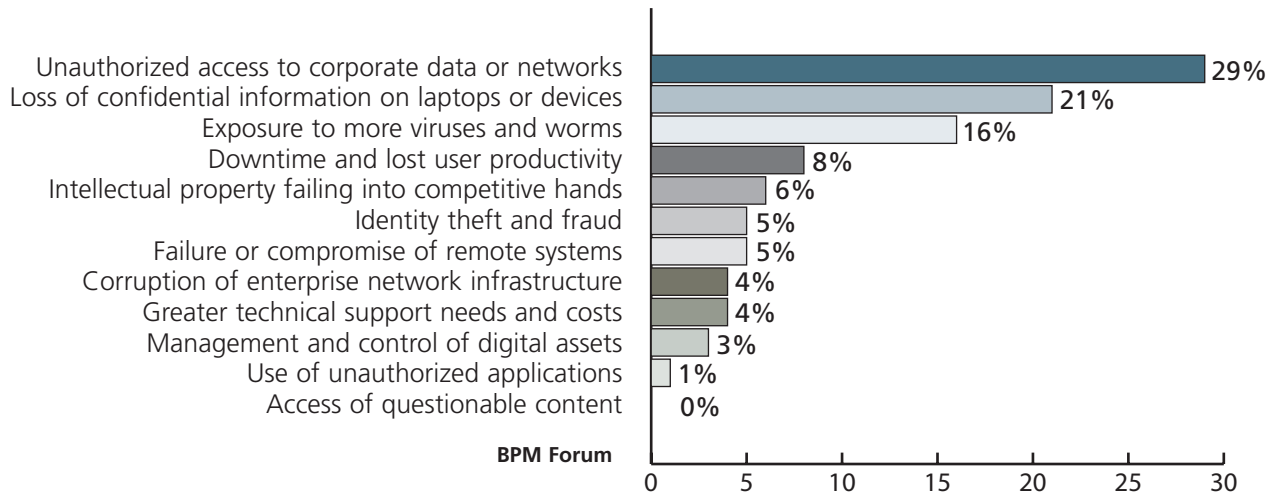
Fifty percent of the executives identified security threats or complexity of applications and operating system software as the items increasing their workload.

Question: What concerns you most about your current help desk operation?



Fifty percent of executives felt their largest concern was getting human intervention at their remote locations on a timely basis.

Question: What is the greatest risk resulting for increased workforce mobility and remote data access from outside the enterprise firewall?



Fifty percent of the executives felt the risks they needed to manage were unauthorized access to corporate data networks and computing devices.

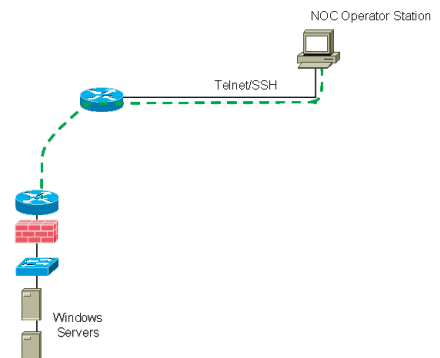
Security and availability of remote locations seems to be on the mind of most IT executives today. It should be with the new regulations around security and the penalties associated with not complying. If that wasn't bad enough, the cost of data theft or poor network performance can impact not only the financial performance of the organization, but the perception of the financial markets as reflected in market capitalization and corporate reputation. The maintenance interface is a big security hole in most remote office environments that needs to be closed before executives experience what TJX did with exposure in every major publication for hackers stealing credit card information from their systems.

How is maintenance access related to intrusion?

Almost every device that is placed into a network has a maintenance console. Windows servers typically use a keyboard, video and mouse. UNIX servers and data communications infrastructure like router, switches and firewalls typically use asynchronous serial connections. Once connected to these maintenance consoles, the operator has total control over that device. The operator can change configurations, extract data, add applications or just about anything else they desire. They have total control over the device. This is the most powerful interface on the equipment and in the wrong hands can result in major security breaches of the kind referred to above.

Access to maintenance interfaces has typically been through Telnet or SSH services either directly to the device or through a terminal server of some kind. These services are on almost all network equipment. They provide cost effective and fast access to the equipment at remote sites for maintenance and configuration. The network operator connects directly to the device over an IP connection, the same IP connection that the application traffic uses. Two problems arise from that:

1. Operators are using the same communication path that has issues to troubleshoot that path. If any portion of the network path is down, the network operator cannot access the device to correct the problem.



2. While it is working fine for the operator, it will work just as well for any intruder attacking the remote location. Intruders utilize ping sweeps where they ping IP addresses across the network sequentially to find out what IP addresses are out there. Once they find them they can utilize a trace route tool to find the path from their device directly to the network element. The example to the right shows how to find devices and the route to get to them. These are standard troubleshooting tools admins use, and they are available to the intruder as well.

```
C:\Documents and Settings\lab-tracet 72.236.162.171
Tracing route to 72.236.162.171 over a maximum of 30 hops
  0  *  *  *  Request timed out.
  1  10 ms  6 ms  7 ms  cpe-76-185-96-1.tx.res.rr.com [66.185.96.11]
  2  7 ms  *  *  GE-1-7-rf02.pilano.tx.dallas.comcast.net [68.87.206.89]
  3  *  *  *  Request timed out.
  4  19 ms  13 ms  14 ms  [24.93.37.101]
  5  15 ms  15 ms  14 ms  be-2-3.car1.Houston1.Level3.net [4.79.98.29]
  6  13 ms  14 ms  14 ms  ae-11-11.car2.Houston1.Level3.net [4.59.132.234]
  7  51 ms  53 ms  54 ms  ae-5-5.ebr1.Atlanta2.Level3.net [4.5.132.236]
  8  72 ms  72 ms  72 ms  ae-2.ebr1.Washington1.Level3.net [4.5.132.236]
  9  65 ms  64 ms  64 ms  ae-14-51.car4.Washington1.Level3.net [4.58.121.171]
 10  65 ms  64 ms  65 ms  TELCOVE INC.car4.Washington1.Level3.net [4.79.168.206]
 11  86 ms  86 ms  86 ms  [24.56.106.85]
 12  88 ms  88 ms  86 ms  [24.56.106.110]
 13  101 ms  89 ms  89 ms  [64.9.103.156]
 14  89 ms  92 ms  89 ms  [72.36.162.171]
Trace complete.
```

Once the intruder has the IP address and the route to the device, all he has to do is issue a Telnet or SSH connection request and he can attach to the network element. Once they break the password, a simple task with sophisticated tools, they are in to the device.

With access to the device, they can do whatever the permissions assigned to that password allows them. Examples of harm they can do are:

- Plant a backdoor that is another password that allows them to come in at will with valid credentials that no one else knows about.
- Adjust routes in routers to send all traffic to the intruder. They then capture the data and send it on to the original location, making the theft transparent to the company.
- Plant malicious code in the form of viruses, trojan horses and worms that will impact the performance of the services. Outages can result for these activities.
- Extract or damage file data with the thought of holding the company hostage with the data or changes. Again, outages can result from these activities.

What is the cost of these activities?

Costs associated with unauthorized intrusion fall into two categories. The two are tangible and intangible. Tangible costs are those that are easily measurable and the impact can be reflected easily and attributed to the activity. Such items are lost revenue; employee productivity loss during an outage or the cost of repairing systems after malicious code has been planted and damaged the system.

Types of Economic Impact of Hack attacks on an Organization

Type of Economic Impact on Organization	Consequences of Impact
Immediate economic impact on a single organization	<ul style="list-style-type: none"> • Damage to systems that require human intervention to repair or replace • Disruption of business operation • Delays in transactions and cash flow
Short-term economic impact on a single organization	<ul style="list-style-type: none"> • Loss to contractual relationships with other organizations in supply chains • Loss of retail sales • Negative impact on the reputation of an organization • Hindrance to the development of new business
Long-term economic impact on a single organization	<ul style="list-style-type: none"> • Decline in market valuation • Erosion of investor confidence • Decline in stock price • Reduced goodwill standing

Source: Computer Economics

More difficult to measure and typically having a far greater impact, are the intangible costs. These are things like the impact on the stock price, the negative impact on market capitalization, potential future litigation and relationships with suppliers and customers. When major intrusions become public the reputation of the company is impacted.

When TJX announced to the market the intrusion into their system the stock price went down approximately three dollars a share. This represented an approximate \$1.3 B decrease. While it has recovered, it is difficult to predict what would have happened without that announcement. Shortly thereafter litigation was announced due to the hacking of credit cards.

These costs have been identified and addressed in the data center for years. With the explosion of the remote office and the dispersion of data across remote office locations, the security hole left through the maintenance interface remains for most organizations. In-band services of Telnet and SSH exposes the organization to attack from both outside and within the organization. As well early implementations of console servers, called data switches, provided connectivity but no ability to secure the remote access of the maintenance console. Forty to fifty percent of executives believe that the largest threat to intrusion is from inside the company and 50% of large organizations have fired staff for security breaches. This places these people inside the firewall, the network element many organizations are relying on to protect them from intrusion. Unless IT departments address the issue of maintenance access to remote sites and the impact on security, they are exposed to unauthorized intrusion.

How can we minimize the impact?

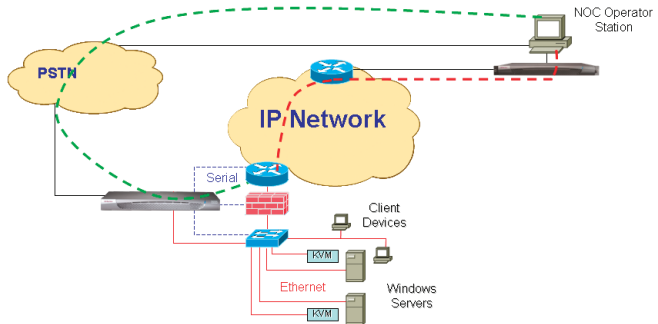
Eliminating any possibility of unauthorized access to remote locations would be optimal. That will most likely never happen. There are a few reasons for this. First the networks and applications are widely deployed and very complex. The IT executive needs to address the entire solution and need to be right 100% of the time. The intruder can focus on a specific area and only has to be successful once. Attackers have all of the same tools as the IT organization and in many cases are more technically competent than the IT organization. Thus the strategy must be a flexible one that makes it more difficult to penetrate the network at each progressive level. The strategy would be that eventually attackers will go somewhere that is easier to penetrate. If hackers do succeed, there needs to be a good audit trail that allows the security organization to see what was done to back out any changes.

Implementing a secure console server instead of in band or early generation data switches can accomplish this task in a very cost effective manner. Placing a secure console server at each remote branch will improve the security by placing major hurdles in the way of the intruder that are not there with in-band solutions such as Telnet and SSH or data switches. Using the secure console server, layers of protection are added to the security plan. As the attacker breaks through each one, he will encounter another that he didn't anticipate and has not encountered in an in-band solution. It will make it many orders of magnitude more difficult to penetrate than the current solutions. Again, it would be nice to guarantee no attacker will penetrate, but for the reasons stated earlier, they have an advantage. Given the time and desire, they will penetrate. All we can do is try to make it as difficult as possible, sending them on to another place that is easier, and tracking their actions if they do succeed.

In addition to improved security, another benefit derived from the implementation is improved troubleshooting tools resulting in lower mean time to repair and higher network availability.

The Layered Security Model

1. **Layer 1** - As mentioned previously, Telnet and SSH talk directly to the network device over an IP connection using the same transport path. By implementing a secure console server (SCS) as shown to the right, Telnet and SSH services can be shut down on the target devices. Any attempt to connect directly to the device, shown in red, will be rejected as the service is not running. The maintenance interface will not be on the same IP address, so the intruder will have a more difficult time finding the interface.

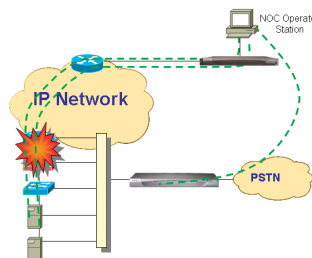
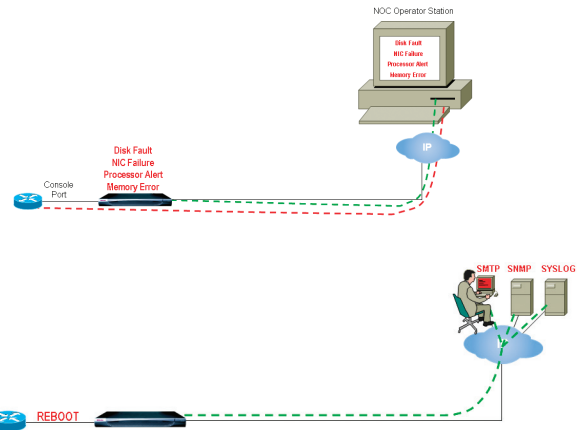
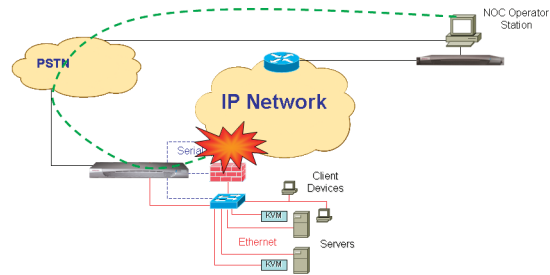


2. **Layer 2** - Should the intruder find the IP address of the SCS, they would normally issue a Telnet or SSH connection request. These services run on standard TCP ports of 23 for Telnet and 22 for SSH. Using a secure SCS, custom TCP ports can be used. Any TCP port out of 65,000 ports can be assigned to Telnet or SSH. Thus when they try to connect using the standard ports 22 or 23, the connection request will be rejected.
3. **Layer 3** - Secure console servers utilize both username and password for access to the device. Based on that username and password, the operator will see only the devices attached to the SCS that they have been authorized to access by the administrator. Using in band or older access methods such as data switches, one password allows access to all devices. With the SCS password architecture, if the intruder accesses the device by repetitive password entry, they will have to find not just the password, but the correct password for the device they are trying to access. Thus operators can be restricted in what they can access. As well, based on that access credential, they will be allowed monitor only, target operation or full administrative permissions. Now they not only have to get the password, but the correct one to access the device they want and the one that allows them to operate the device.
4. **Layer 4** - Should the intruder have the patience and take the time to find the correct TCP port, they then need to log in. Most devices support standard passwords with little or no rules associated with them. With the strong password support on the SCS, the administrator can specify minimum and maximum length, the construction of the password with letters, numbers and special characters, expiration periods for passwords and the number of new passwords until one can be reused. This will make it much more difficult for the sophisticated software hunting for the password to find it.
5. **Layer 5** - As they are searching for the password, there is a counter that states how many tries can be made before the attempt is blocked. As well there is a parameter that states how long they will be blocked. Thus if the invalid attempts are exceeded, that users IP address is blocked until the timer expires. This function will make it even more difficult to gain access.
6. **Layer 6** - If all of the five layers are penetrated, there is one dedicated attacker and they are into the system unauthorized. Now, based on the permissions in the SCS, the attacker will only be able to gain access to the targets assigned to that password. If they guess the password with permission to access the router and wanted to go to the server, they will have to start the password search again.
7. **Layer 7** - If they get to the local console port of the target device, they will once again need to authenticate with that device all over again. This is where they would have started with an in-band solution such as Telnet or SSH.

- Layer 8** - By placing all of the additional layers of protection in the way of a successful intrusion, there is a very good chance the attacker has gone elsewhere. If not and they gain access to the target, the SCS logs all of the activity based on each keystroke to an external server. Whatever the intruder does will be recorded so that when the incursion is discovered there will be a record to facilitate repairing whatever was done to the target. As well, SCS normally supports SYSLOG and records all major events such as login, logout and configuration changes. This will aid in identifying who accessed the devices and when.

Improving Network Availability

- Dial Access** - Implementing an SCS improves the ability of the operations people to troubleshoot faults in the network. With in-band solutions, if the network fails, the operator is unable to connect via the network because it has failed. With the right SCS the operator can get dial access to the SCS and troubleshoot the devices and is not locked out of the remote location. As an additional security layer, dial back is available. Once a user dials in and is authenticated, his call is disconnected. The SCS then dials back to a preconfigured number. This insures that not only is the person authorized, but that they are at the appropriate location. Someone can't falsely get a number and password and connect. They also need to be at the approved telephone number to have access.
- Console Message Storage** - Devices with console ports will send messages to the console port when problems occur. Having these messages facilitates troubleshooting. With in-band solution if the operator isn't attached to the device the messages are lost. Placing the SCS at the location will store those messages and when the operator connects, they will be able to display them.
- Console Message Alerts** - Certain messages can be specified that will cause the SCS to send an alert to one of three places. Alerts can go to SYSLOG or an SNMP collector or to specified e-mail addresses for immediate action.
- Power Management** - Using in-band techniques, there is no facility for controlling power for the devices at the remote location. Should a device hang or the network go down, a call to the remote must be made. Someone needs to talk a person at the site through power cycling the equipment. With a SCS at the site a connection through the leased line or dial service will allow the operator to cycle the power on individual devices, thus giving them a hard restart.



Summary

The continuing reliance on network technology for business performance improvement is causing IT executives to consider how to better maintain the availability of the network and to provide added security. With more data being transported to or residing at the locations, security of this data becomes all the more important. Existing techniques for accessing maintenance consoles leave security holes in the network and are not the most efficient in reducing mean time to repair. The costs associated with outages and security breaks can be huge. By deploying a secure console server, maintenance consoles can be secured and the availability of the network improved.

About Raritan

Protecting availability and security of networks for remote locations against changing security threats is a never-ending task. Raritan is the best choice for partnership in pursuing this goal because it is a forward-looking, security-aware company with extensive experience in providing Serial Console Solutions. Raritan addresses current and potential security problems with a disciplined approach to architecture and an innovative approach to engineering.

Raritan's Dominion SX serial console server is a secure, out-of-band remote management solution with maximum security and integrated power control.

Raritan's Dominion XRO is a secure, remote, out-of-band access and power control of servers and other network devices over IP.

Raritan provides innovation and a "best practices" mind-set at the architectural level, from the beginning of every product's design phase. The use of formal modeling techniques in designing SCS, the adoption of Open Source components in implementing those solutions, and the level of importance assigned to human factors, together provide much greater assurance that Raritan's distributed system security mechanisms will work as intended.

References:

The Remote Revolution. The BPM Forum. GlobalFluency. December 2005.

Cisco ROI for Network Security. Cisco Systems, Inc.

End users behaving badly : Threats from the inside. IDC. January 2007.