Locking Down Vendor Privileged Access Within Your Network

Sponsored by: SecureLink
7/9/19

SPEAKERS

Justin Strackany

Justin Strackany is the **Chief Customer Officer at SecureLink**, the leader in vendor privileged access. He has been with SecureLink since it was founded in 2003 and has served in many customer-focused capacities, including sales engineering, implementation, customer success, account management, and onboarding new clients. Over the years he has developed deep partnerships with some of the largest, most complex enterprise organizations and technology vendors across the country and internationally in industries such as healthcare, gaming, legal, finance, and retail.

Tony Howlett

Tony Howlett is a published author and speaker on various security, compliance, and technology topics. He serves as President of (ISC)2 Austin Chapter and is an Advisory Board Member of GIAC/SANS. He is a certified AWS Solutions Architect and holds the CISSP, GNSA certifications, and a B.B.A in Management Information Systems. Tony is currently the **CISO at SecureLink.**

How to secure vendor privileged access to your network and ensure compliance

Current State

- As organizations become more specialized they are relying more on third-party technology vendors to handle critical applications and infrastructure
- Vendor users often have privileged access with little accountability
- Vendors should be treated differently than your internal or remote employees
- Right person, right access, right time

Business Risk Imposed by Data Breaches

A company's reputation established and nurtured for 100 years can suffer severe and lasting damage following just one high-profile cyber attack. As a result, it can be difficult for boards to feel fully confident in how they are monitoring cybersecurity risk, both within the organization and especially among vendors

Scott Laliberte, Managing Director, Global Leader, Security and Privacy Practice, Protiviti

Major Breaches Caused by Third-Parties

COMPANY	EVENT	# OF RECORDS	ROOT CAUSE
LabCorp/Quest	Customers billing (CC# etc.) and services rendered	20,000,000	Collection agency hacked
MyHeritage.com	Customer pws and emails released	92,000,000	Payment processing vendor hacked
MyFitnessPal.com	Customer emails, username and pw stolen, access to PHI	150,000,000	Security vulnerability in acquired business unit
Hard Rock Casino	Credit card data over three separate breaches	Unknown; 7 months of transactions (est to be 800,000)	POS system in 2015 and 2016; Sabre system in 2017

State & Local Governments Hit Hard

The New York Times

Hit by Ransomware Attack, Florida City Agrees to Pay Hackers $600,000

The city council in Riviera Beach, Fla., voted quietly to authorize a nearly $600,000 ransom payment after hackers paralyzed the city's computer systems.
Wilfredo Lee/Associated Press

Second Florida city pays giant ransom to ransomware gang in a week

Lake City officials give in and agree to pay nearly $500,000 to ransomware gang.

By Catalin Cimpanu for Zero Day | June 26, 2019 -- 07:44 GMT (00:44 PDT) | Topic: Security

Third Florida city falls victim to ransomware attack

Stop clicking on email links, city employees

By **Rob Thubron** on July 1, 2019, 9:34 AM | 8 comments

June 28, 2019

Baltimore approves $10M for ransomware relief, expects $18M in damages

Robert Abel

Follow @RobertJAAbel

Ryuk, Ryuk, Ryuk: Georgia's courts hit by ransomware

It looks like another Ryuk ransomware campaign is responsible.

SEAN GALLAGHER - 7/1/2019, 3:52 PM

rs / Wikimedia

85.4 GB of Security Logs Exposed

CYBER SECURITY NEWS

Third Party Data Breach to Blame for Data Leaks of Major Hotel Chains

Scott Ikeda — On **Jun 10, 2019**

- Sometimes it's not just customer/client data that can get exposed
- Internal/HR records and emails, 3rd or 4th party data

Business Risks Imposed by Third-Party Vendors

- **Operational risk:** Average of 6 outages a year to critical business systems
- **Security risk:** Thousands of users connecting in with full access to the network and shared credentials
- **Financial & Reputational risk:** Global average cost of a data breach is up 6.4 percent over the previous year to $3.86 million.
- **Compliance and Regulatory risk:** You are responsible for securing your vendors with access to regulated data or systems. Being in violation of regulations can result in fines, operational limitations and even criminal liability for officers, even if a vendor caused the breach.

Nth Party Risk

- Nth party vendors multiply risk
- It only takes a breach of one of these parties for bad actors to get into your system

Reputational Risk for Legal Organizations

- Small firms reputation can be greatly damaged by a vendors mistake
- Losing client trust can be devastating
- Insurance policies and legal recourse against a vendor can not replace that.

Recently in the News …

AMCA Files Chapter 11 After Data Breach Impacting Quest, LabCorp

After an eight-month data breach impacted up to 20 million patients of Quest Diagnostics, LabCorp, and BioReference, AMCA has filed for Chapter 11 protection – aiming to liquidate.

The Challenge with Vendor Management

The Third-Party Access Tsunami

- 67 vendors
- 238 customers
- Multiple users
- 63% of data breaches
- Unlimited risk
- Increased risk leads to stricter regulatory requirements
- Reliance on a higher number of third-party technologies

Compliance and Regulations

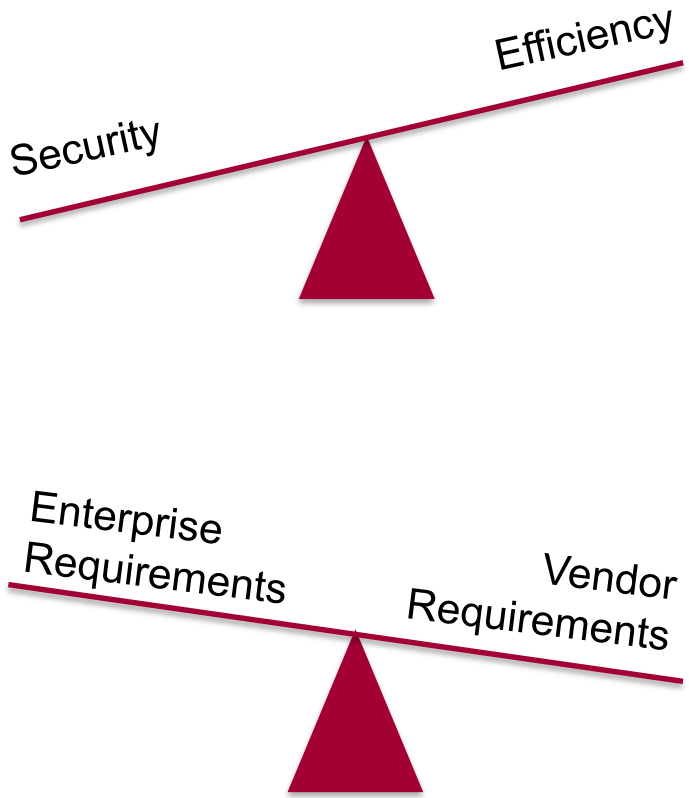
- While compliance regulations vary by industry, there are key remote access standards and best practices that every sector must review

Common Challenges for Legal Organizations

- Managing multiple compliance regulations
- Access management and control
- Authentication and authorization
- Audit

Barriers to a Robust, Efficient Third-Party Remote Access Solution

- Lack of resources or budget
- Multiple solutions to manage
- Wrong tool for the job
- Application owner challenges
- Vendor buy-in



Legal, Privacy, and Security Best Practices for New Vendors

Legal Considerations

- Due Diligence: Before contracting and ongoing
- Contract - Exclusions, amendments and additions
- Regulatory - May be required to bind vendors to the same requirements of regulated entity
- Termination - What happens after the relationship ends?

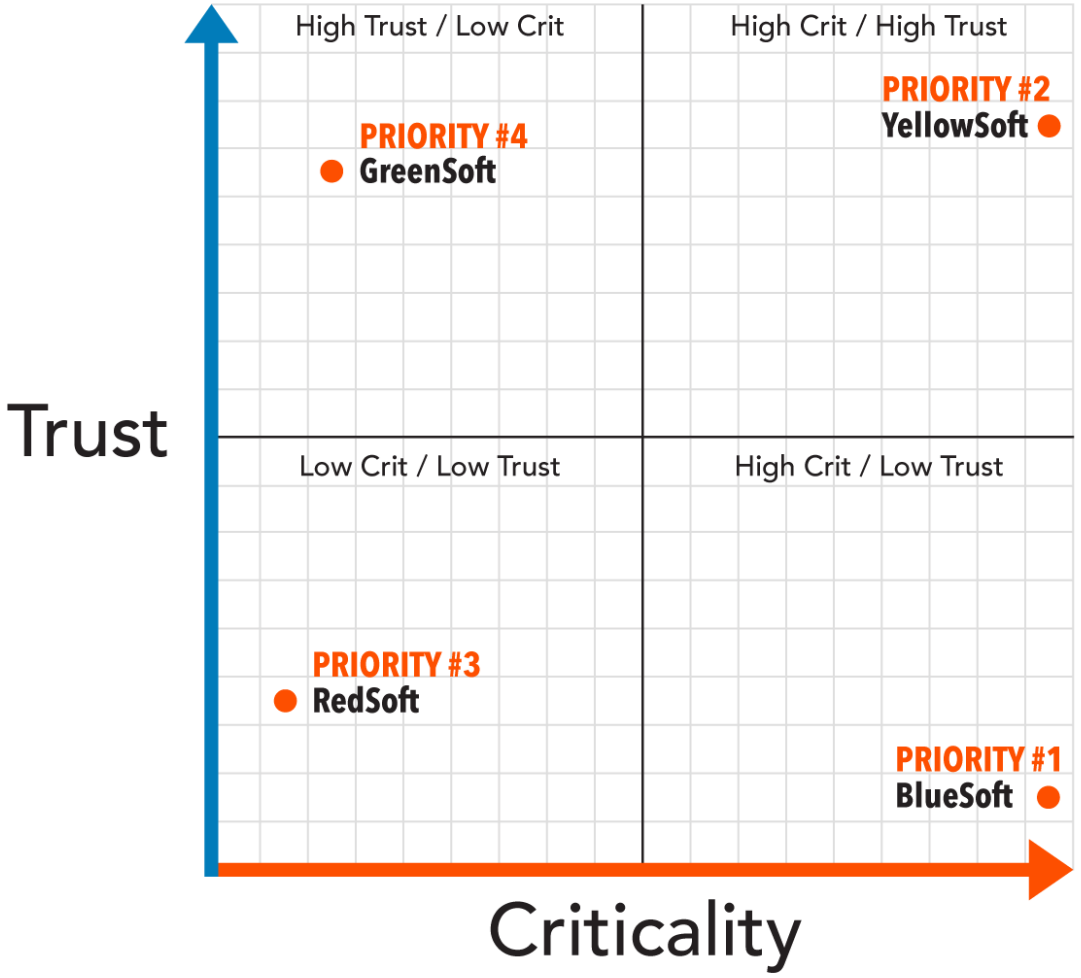
Due Diligence

- What is goal of relationship?
- What services expect to receive?
- What data will be shared, generated, used, held, or more by vendor?
- What is vendor’s standing with regulatory requirements?

Due Diligence

- Sample considerations:
  - When was last risk assessment conducted?
    - What were results?
  - What policies and procedures are in place?
  - What certifications are held?
  - When was last breach and what was scope of issue?
  - Are exclusion checks run?

Vendor Risk Assessment - Tiering



The Contract

The Contract: Key Considerations

- Indemnification
- Insurance
- Fees
- Termination Rights
- Data Rights and Usage

Regulatory Issues

- In healthcare, HIPAA/HITECH regulations drive and influence many decisions
- Should factor into and shape vendor relationships
- New privacy laws have data governance requirements for third parties (GDPR, CPPA)
- Others on the way...

Ending the Relationship

- First, look to the contract
  - Termination provisions can provide framework
- Second, look at regulations
  - For example, HIPAA does not allow broad right of retention
- Third, review internal policies

Ending the Relationship

- Additional Considerations
  - Will transition assistance be provided or is it needed?
  - How long will files, analyses, or other deliverables be retained?
  - Will any services continue past the effective date of termination?
  - Do any claims or liabilities between the parties exist?

Security and Compliance Best Practices for Your Current Vendors

Security and Compliance Best Practices

Identify and Authenticate

Control Access

Record and Audit

Identifying Your Vendors

Impact on Identity – Shared Accounts

- Unable to tie actions to individuals
- Common attack vector
  - Target data breach
- Terminated employees retain access
- Limited accountability

Best Practices for Identifying Vendors

- Eliminate shared credentials
- Tie actions to individual users
- Termination protocols

Controlling Your Vendors

Insufficient Access Controls

- Increases exposure of sensitive data
- Increases potential impact of mistakes
- Increases magnitude of potential breach
- Difficult to enforce access policies

Best Practices for Controlling Vendor Access

- Management of permissions (Least Privileged Access)
- Delegate access controls to appropriate users

Auditing Your Vendors

Limited Audit

- Lowers compliance standards
- Fails to hold vendors accountable
- Limits policy enforcement
- Prevents deeper forensics

Best Practices for Auditing Your Vendors

- Video recording of sessions
- Obtaining contextual information upon access to tie actions down to individuals

Context is King

- Important to acquire the contextual information you need prior to vendor connection
- Should be compliant and easily translated into audit logs

Common Options for Remote Support

Desktop Sharing and VPN

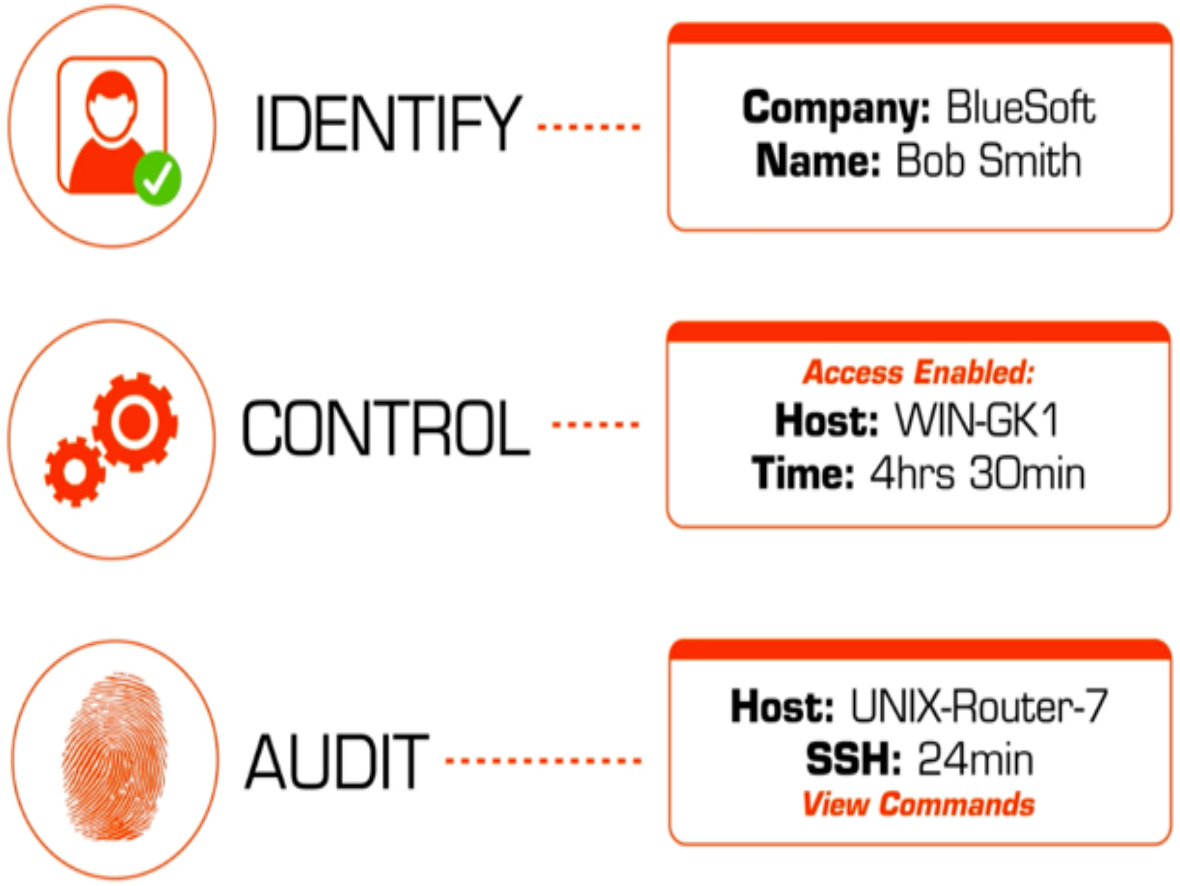
01	VPNs	Great for employees but not ideal for third-parties since they lack the ability to identify, control and audit third-parties
02	Desktop Sharing	Great for attended desktop support and helpdesk, but lack the security and functionality needed for complex remote support
03	PAM Solutions	Good for managing privileged credentials but require additional technologies for comprehensive remote access security

Security Automation

Optimizing Security Headcount

- With data breaches on the rise, increasing security is critical
- How do you increase security with your existing staff?
- Many organizations struggle with balancing needs

Introducing VPAM – Vendor Privileged Access Management



What Makes SecureLink Different

- Purpose-Built for Vendor Management
- Supports Highest Compliance and Security Standards
- Supports Enterprise-Grade Remote Access
- Fast Time to Value with All-in-One Offering

Your Partner for Vendor Privileged Access

Focused solely on secure vendor privileged access for highly regulated industries

Support more than 30,000 organizations worldwide

www.securelink.com
contact@securelink.com
888.897.4498

Have questions?

contact@securelink.com
888.897.4498

SECURELINK
VENDOR PRIVILEGED ACCESS