SecurityScorecard

venminder

Third-Party Cyber Risks Are Increasing – Better Bring Your A-Game

September 15th 2020

Housekeeping

Recording

Discussion + Q&A

Agenda

- Speaker Introductions
- Vendor Risk Management Lifecycle
- Cybersecurity & the Impact of COVID-19
- Cybersecurity Documents & What to Look For
- Key Cybersecurity Red Flags
- Mitigating Cybersecurity Risk and Best Practices
- Q&A

Speakers

Alex Heid

Chief Research & Development Officer

SecurityScorecard

Gordon Rudd, CISSP

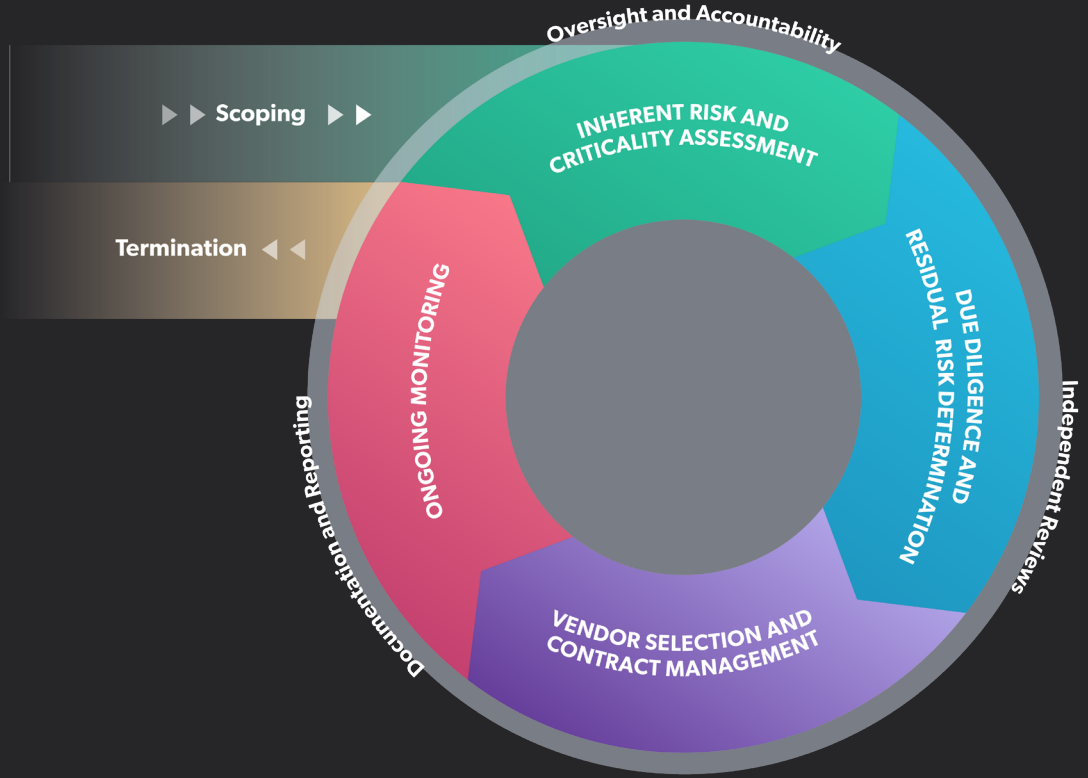
Third-Party Risk Officer

Venminder

Vendor Cybersecurity

Is your vendor prepared to prevent, detect and respond to a cybersecurity threat?

Vendor Risk Management Lifecycle

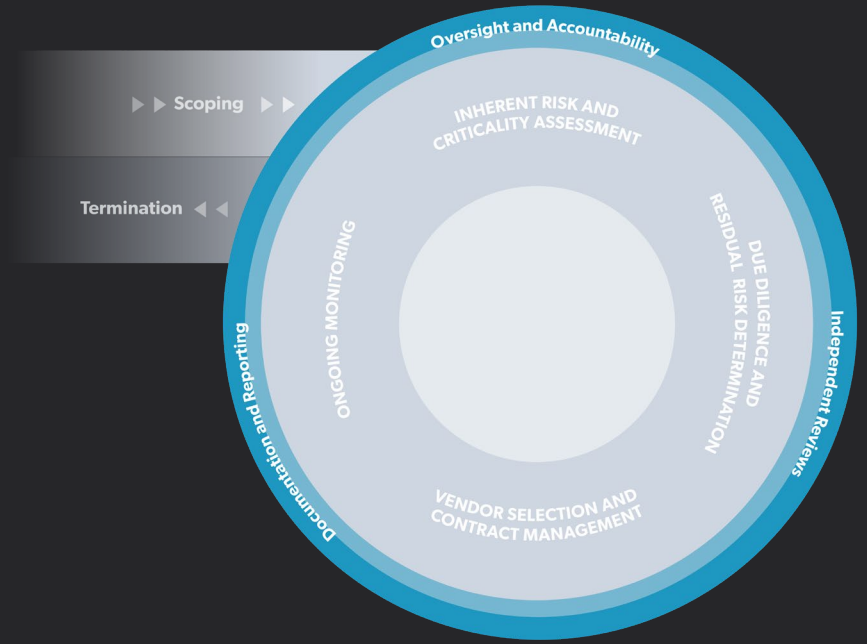


Where Cybersecurity Fits In

Guiding the Lifecycle

Documentation & reporting, oversight & accountability and independent review are peripheral to, but an integral part of the third-party risk management lifecycle. Cybersecurity should be considered in all of these.

- Governance documents
  (i.e. policy, program and procedures)
- Document everything
- Cybersecurity will be part of reports prepared
- Internal audit team – they will review cybersecurity

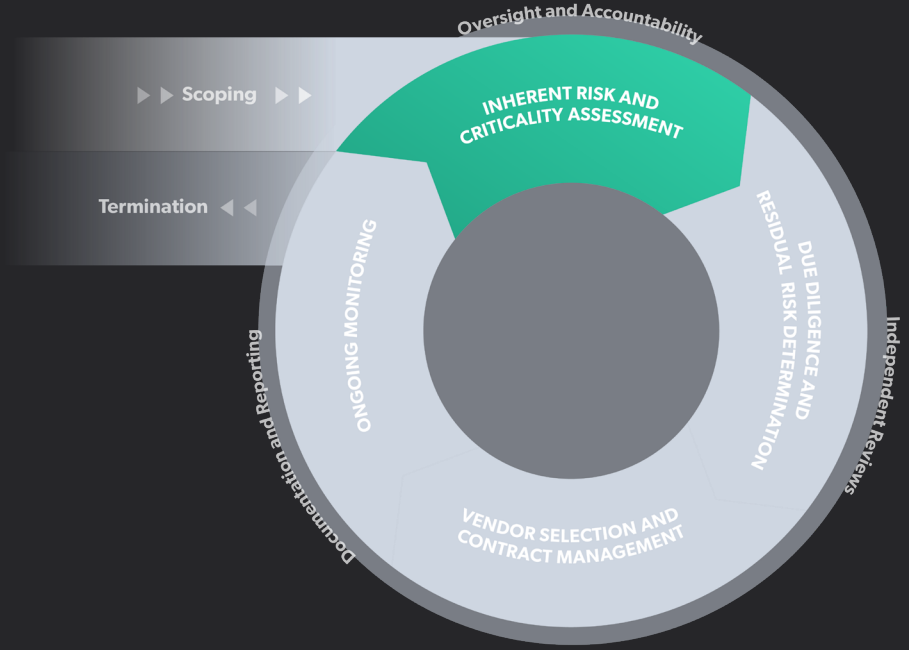


Where Cybersecurity Fits In

Inherent Risk and Criticality Assessment

A strong risk assessment process is vital to a comprehensive third-party risk management program.

- Analyzing cybersecurity posture for new and ongoing vendor relationships
- Helps with discovering cybersecurity risk from outsourcing
- Makes you aware of faulty cybersecurity controls

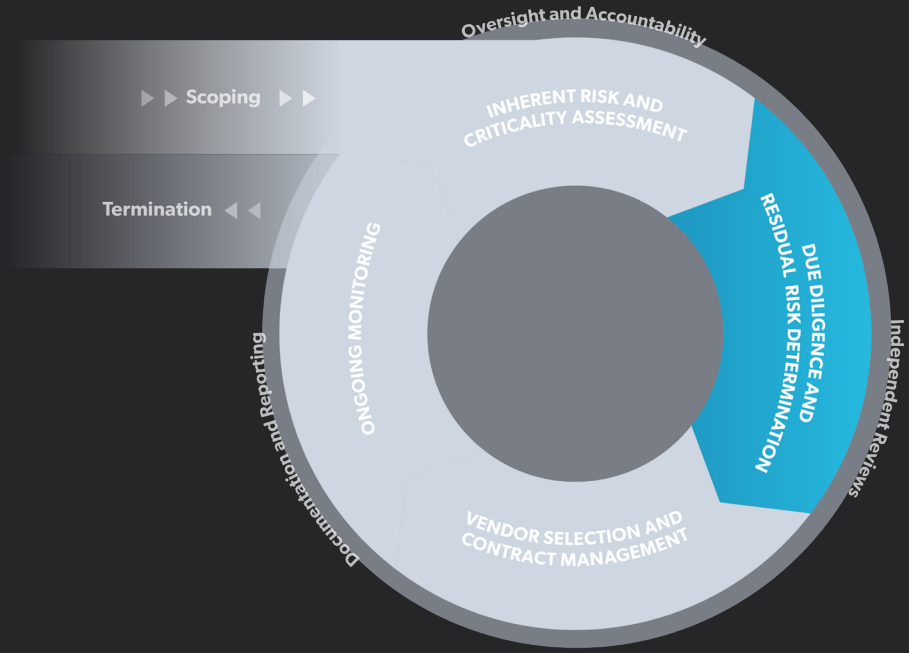


Where Cybersecurity Fits In

Due Diligence and Residual Risk Determination

Due diligence is one of the most important activities in third-party risk management.

- Collecting cybersecurity documentation
  - SOC Reports
  - Vulnerability Tests
  - Penetration Tests
  - Data Retention and Destruction Policies
  - Business Continuity Plans

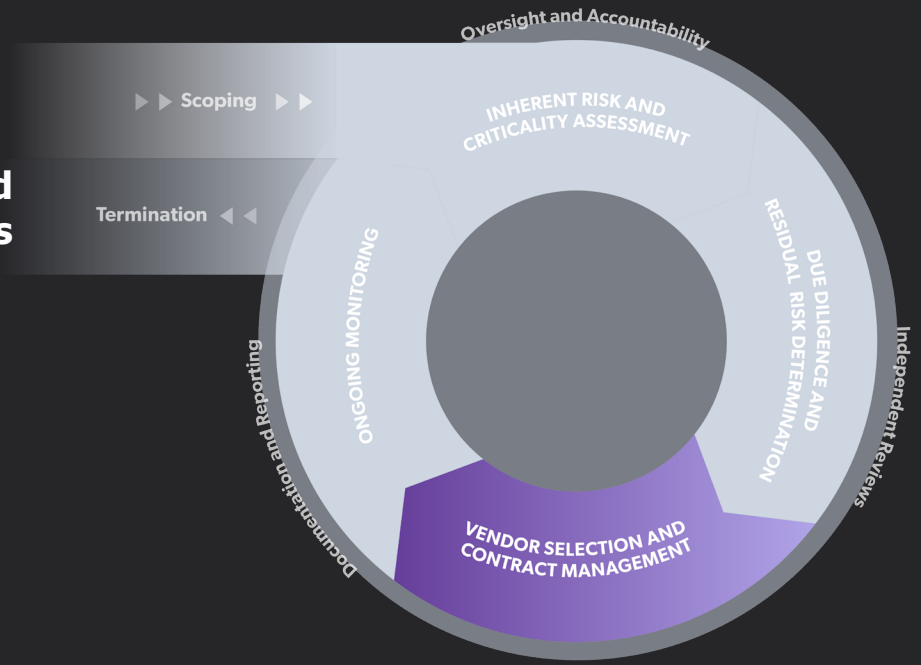


Where Cybersecurity Fits In

Vendor Selection and Contract Management

Choose the best vendor and administer sound written agreements. Spot cybersecurity items in the contracts and set related SLAs.

- Accessibility to cyber policies and procedures
- Independent testing requirements
- Availability of test results and reporting
- Recovery times
- Back-up responsibilities
- Breach/disruption notification
- What happens to the data assets

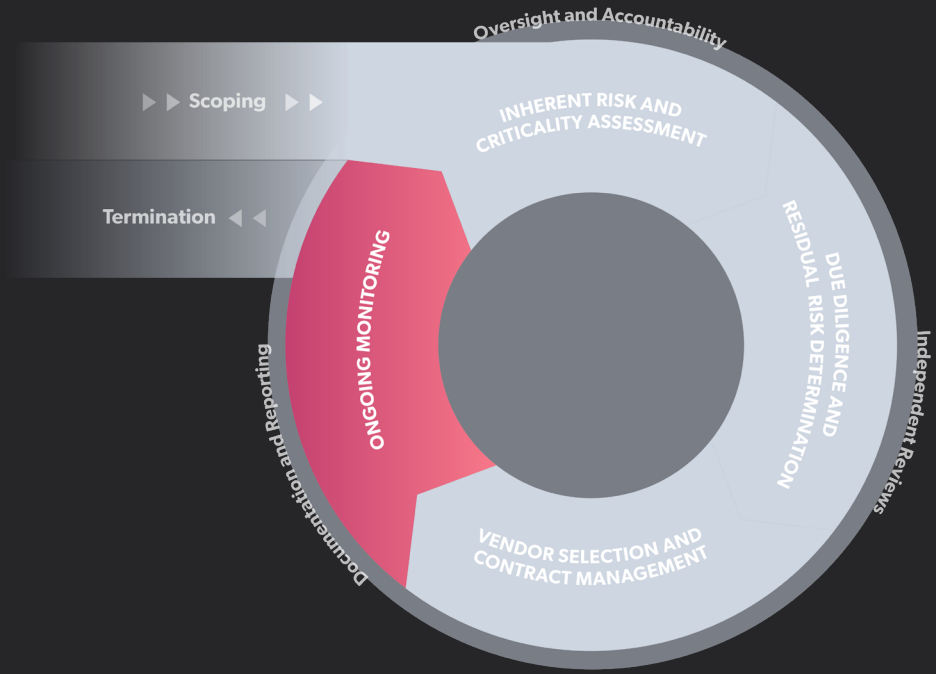


Where Cybersecurity Fits In

Ongoing Monitoring

Keep abreast of a vendor's performance and well-being throughout engagement and continued periodic assessments.

- Verify vendors still meet cybersecurity expectations
- Identify areas of cybersecurity concern
- Discover any cybersecurity gaps or cybersecurity related items they said they would do but aren't

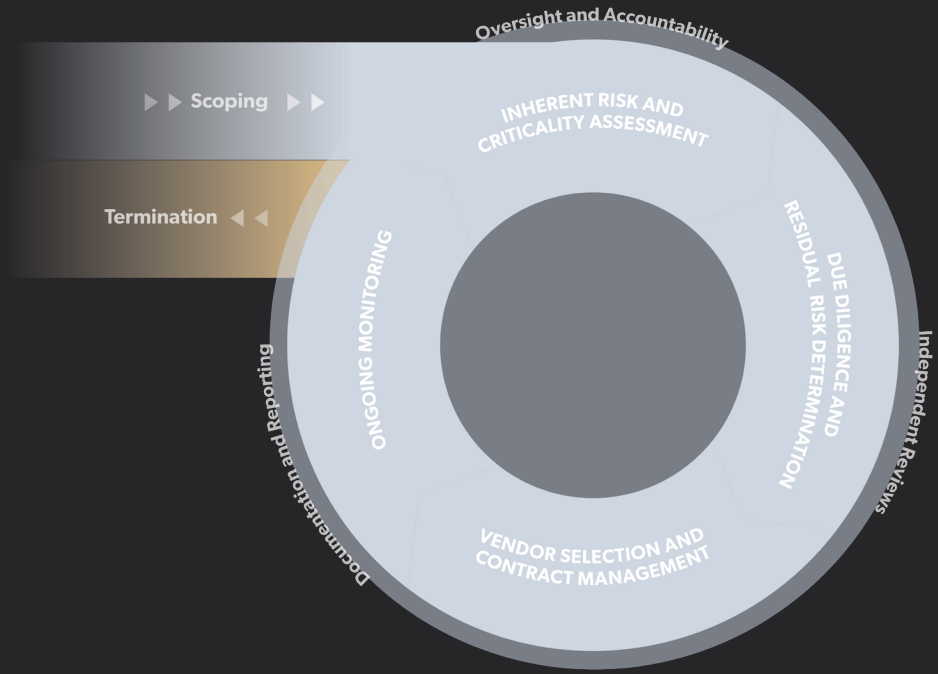


Where Cybersecurity Fits In

Termination

If the vendor relationship has come to an end:

- Ensure exit strategy requirements established in the contracting stage are met



Cybersecurity and the Impact of COVID-19

Working remotely created new attack surfaces for cybercriminals to exploit

- Remote workers often lack secure equipment and protocols that provide robust digital controls and compliance
- It's estimated that 1/3 of the American workforce will be working remotely by the end of 2021
- Increased reliance on cloud-based communication
- Infrastructure AND resources spread thin

Regulators are watching

- How are you handling these new risks?
- How are you ensuring your VENDORS are handling the new risks?

What Cybersecurity Documents Do You Collect?

- SOC reports
- Business Continuity Plans
- Network Penetration and/or Vulnerability Assessment
- Intrusion Detection/Incident Response Plans
- Data Retention and Destruction Policies
- Data Classification and Privacy Policies
- Employee, Contractor and Vendor Management Confidentiality Agreements and Security Training

What Are You Looking For?

- **SOC Reports**
  - The scope of the system and the engagement
  - List of User Entity Controls Considerations
  - List of controls tested
  - Exceptions [if any]

What Are You Looking For?

- **Business Continuity Management Plans**
  - Pandemic planning
  - Mobile device management (MDM) and connectivity standards
  - Remote workforce guidelines for data
  - Personal device management guidelines
  - Endpoint protection & patch management
  - Ongoing employee education
  - Incident response
  - Crisis management

What Are You Looking For?

- **Security Testing**
  - Internal and External Vulnerability Testing
  - Penetration Testing
  - Social Engineering
- **Sensitive Data Security**
  - Encryption
  - Data Retention and Destruction policies
  - Data Classification and Privacy Policies
- **Cybersecurity Insurance Coverage**
  - Verifying the vendor has cybersecurity insurance coverage

What Are You Looking For?

- **Employee, Contractor and Vendor Management**
  - Confidentiality Agreements
  - Security Training
  - Access Management Policies
- **Incident Detection and Response**
  - Including incident notification clauses within your contract
  - Reviewing the incident management plan to ensure it's comprehensive

SOC for Cybersecurity

Intended to be used when interested in validating that the cybersecurity risk management program is designed and operating effectively. Not mandatory, but nice if a vendor has one.

The 3 Components of a SOC for Cybersecurity Report

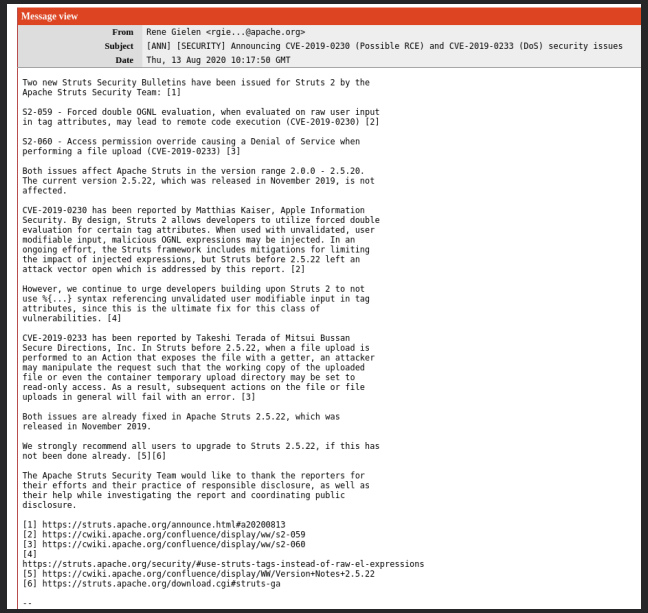
1. Management's Description
2. Management's Assertion
3. Auditor's Opinion

Key Cybersecurity *Red Flags* to Monitor on a Continuous Basis

- Time to patch. How long between a software patch being issued and the patch being applied?
- Legacy systems: How many legacy systems are in production?
- Time to remediate. For issues like malware detection, once an infection is known, how long does it take to get fixed?
- Uniformity. Does a company have 10 issues with a single version, or 10 issues over 10 versions?
- Default Configurations: Does a company ensure that newly deployed systems have had default configurations changed? Have default passwords been changed/removed?

Apache Struts2 Updates in 2020

- How long does it take to implement a software patch from the time it has been issued?



Message view

From	Rene Gielen <rgie...@apache.org>
Subject	[ANN] [SECURITY] Announcing CVE-2019-0230 (Possible RCE) and CVE-2019-0233 (DoS) security issues
Date	Thu, 13 Aug 2020 10:17:50 GMT

Two new Struts Security Bulletins have been issued for Struts 2 by the
Apache Struts Security Team: [1]

S2-059 - Forced double OGNL evaluation, when evaluated on raw user input
in tag attributes, may lead to remote code execution (CVE-2019-0230) [2]

S2-060 - Access permission override causing a Denial of Service when
performing a file upload (CVE-2019-0233) [3]

Both issues affect Apache Struts in the version range 2.0.0 - 2.5.20.
The current version 2.5.22, which was released in November 2019, is not
affected.

CVE-2019-0230 has been reported by Matthias Kaiser, Apple Information
Security. By design, Struts 2 allows developers to utilize forced double
evaluation for certain tag attributes. When used with unvalidated, user
modifiable input, malicious OGNL expressions may be injected. In an
ongoing effort, the Struts framework includes mitigations for limiting
the impact of injected expressions, but Struts before 2.5.22 left an
attack vector open which is addressed by this report. [2]

However, we continue to urge developers building upon Struts 2 to not
use %{...} syntax referencing unvalidated user modifiable input in tag
attributes, since this is the ultimate fix for this class of
vulnerabilities. [4]

CVE-2019-0233 has been reported by Takeshi Terada of Mitsui Bussan
Secure Directions, Inc. In Struts before 2.5.22, when a file upload is
performed to an Action that exposes the file with a getter, an attacker
may manipulate the request such that the working copy of the uploaded
file or even the container temporary upload directory may be set to
read-only access. As a result, subsequent actions on the file or file
uploads in general will fail with an error. [3]

Both issues are already fixed in Apache Struts 2.5.22, which was
released in November 2019.

We strongly recommend all users to upgrade to Struts 2.5.22, if this has
not been done already. [5][6]

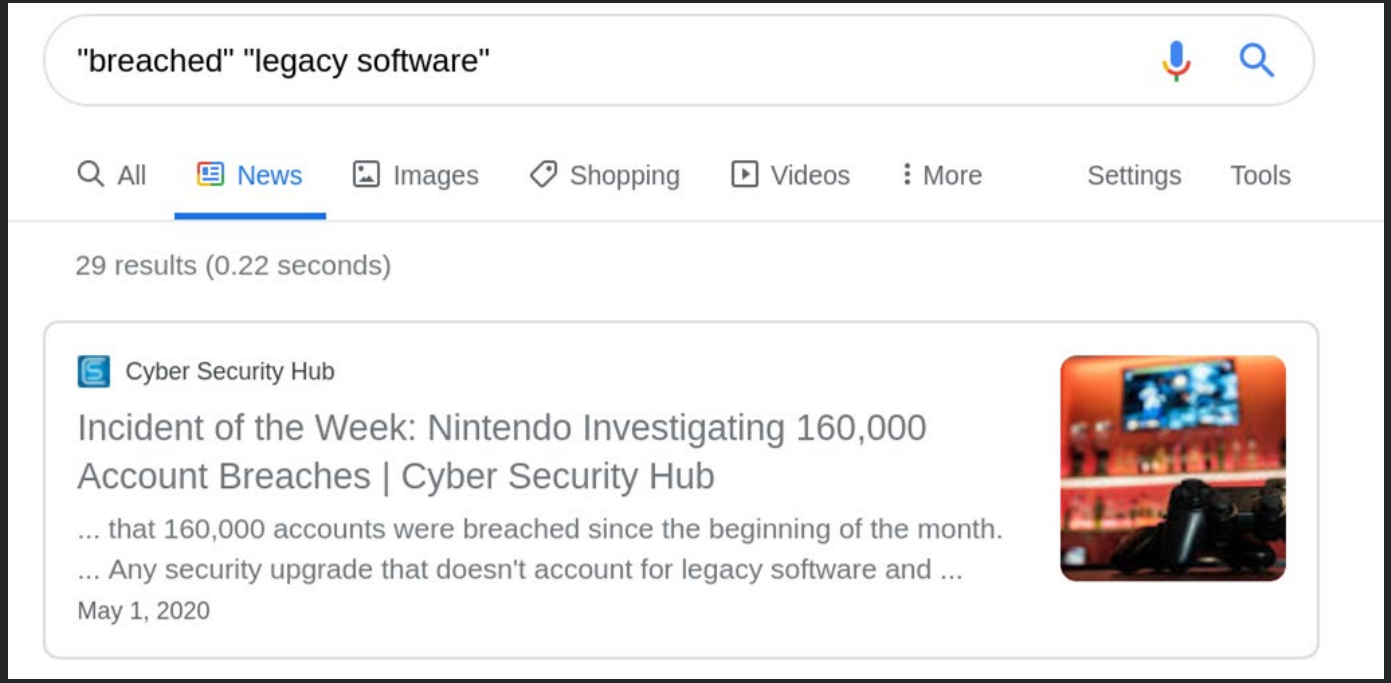
The Apache Struts Security Team would like to thank the reporters for
their efforts and their practice of responsible disclosure, as well as
their help while investigating the report and coordinating public
disclosure.

[1] https://struts.apache.org/announce.html#a20200813
[2] https://cwiki.apache.org/confluence/display/ww/s2-059
[3] https://cwiki.apache.org/confluence/display/ww/s2-060
[4]
https://struts.apache.org/security/#use-struts-tags-instead-of-raw-el-expressions
[5] https://cwiki.apache.org/confluence/display/WW/Version+Notes+2.5.22
[6] https://struts.apache.org/download.cgi#struts-ga

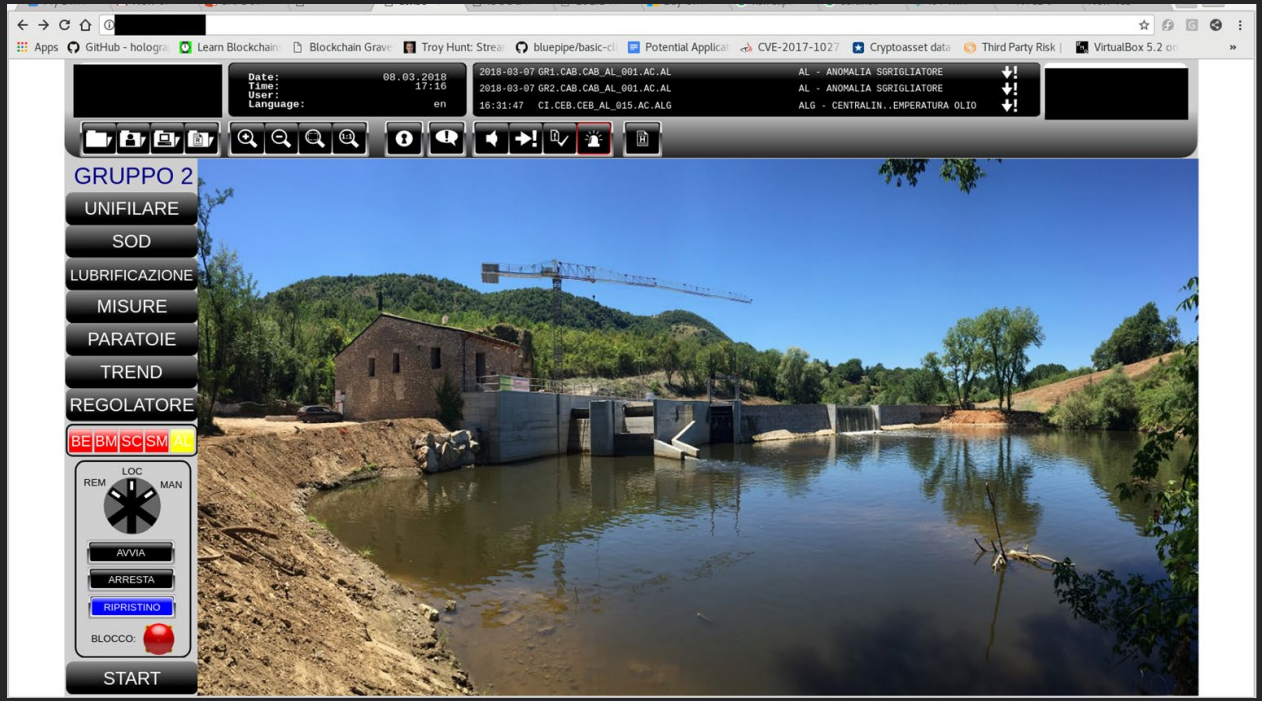
--

Thu, 13 Aug 2020 10:17:50 GMT

Legacy Systems as a Breach Vector



Misconfigurations as a Breach Vector



What to Do If a Vendor Has Poor Cybersecurity Posture

1. Ramp up vendor oversight
2. Have an alternate vendor option available
3. Review the incident management plan
4. Confirm your organization's cybersecurity insurance coverage
5. Use data encryption
6. Review the vendor's data retention policies, destruction policies, data classification and privacy policies
7. Ask for copies of security tests (vulnerability testing, penetration testing and social engineering)
8. Review/use exit strategy - SLAs recourse to exit

Mitigating Cybersecurity Risk

If you identify a cybersecurity risk with a vendor:

- Reach out to the vendor and ask them to address and strengthen controls
- Increase ongoing oversight and write additional oversight requirements into the contract renewal
- Start seeking alternative vendors if the issue isn't resolved in a timely or effective manner – be prepared!

Mitigating Cybersecurity Risk

5 Areas to Review Thoroughly:

- Risk Management and Oversight
- Threat Intelligence and Collaboration
- Cybersecurity Controls
- External Dependency Management
- Cyber Incident Management and Resilience

Consequences of Not Properly Monitoring Vendor Cybersecurity

- Data breach
- Reputation damage
- Loss of customer confidence
- Compliance issues (enforcement actions, fines, etc.)
- Financial loss

Best Practices in Managing Vendor Cybersecurity Risk

1. Make sure your vendors have an *active* SETA program (Security Education, Training & Awareness)
2. Know your vendors' 5 P's - policy, procedures, processes, projects & people
3. Understand the vendor's security architecture
4. Ensure vendors have a business continuity management plan
5. Incorporate cybersecurity in risk management processes for ALL critical and high-risk vendors
6. Verify vendors are providing cybersecurity training & cross-training

Q&A

SecurityScorecard

Thank You