How healthcare leaders can avoid data breaches

Christopher Killion
Healthcare Solutions Architect
ServiceNow
Agenda

• State of healthcare
• Methodology
• Ponemon Research key findings:
  – The Patching Paradox: Broken processes means more people does not equal more security
  – Important factor in reducing risk of breach for healthcare organizations
• Impact to healthcare
• Recommendations
## Current state of healthcare

<table>
<thead>
<tr>
<th></th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Global pandemic</td>
</tr>
<tr>
<td>2</td>
<td>Telehealth workforce</td>
</tr>
<tr>
<td>3</td>
<td>Patient confidence</td>
</tr>
</tbody>
</table>
Security breaches in healthcare continue to rise

2019 to present, the US Dept. of Health and Human Services reported these breaches across the US, with hundreds of thousands of individuals affected.

Source: US Departments of Health and Human Services.
Teams are understaffed and overwhelmed

- Too many alerts
- Manual processes
- Siloed organizations
ServiceNow commissioned the Ponemon Institute to survey nearly 3,000 IT security professionals, of which 258 respondents were from healthcare institutions. Respondents were based in Australia, France, Germany, Japan, the Netherlands, New Zealand, Singapore, the United Kingdom, and the United States, and represent companies with more than 1,000 employees.

### COUNTRIES SURVEYED

<table>
<thead>
<tr>
<th>Country</th>
<th>Total Respondents</th>
<th>% HC</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>595</td>
<td>11%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>387</td>
<td>9%</td>
</tr>
<tr>
<td>Germany</td>
<td>453</td>
<td>11%</td>
</tr>
<tr>
<td>France</td>
<td>369</td>
<td>11%</td>
</tr>
<tr>
<td>Netherlands</td>
<td>340</td>
<td>11%</td>
</tr>
<tr>
<td>Australia/New Zealand</td>
<td>220</td>
<td>10%</td>
</tr>
<tr>
<td>Singapore</td>
<td>165</td>
<td>12%</td>
</tr>
<tr>
<td>Japan</td>
<td>394</td>
<td>11%</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>2,923</strong></td>
<td><strong>322</strong></td>
</tr>
</tbody>
</table>

Margin of Error: 4.51%
Publicized data breaches are just the top of the iceberg

53% of healthcare organizations had one or more data breaches in the last two years

$429

Per healthcare record compared to the average of $150*

*Source: Ponemon 2019 Cost of Data Breach Study
Severity and volume of cyberattacks continue to rise

- 53% of healthcare organizations experienced one or more data breaches in the last two years
- 26% Increase in cyberattack severity over the last 12 months
Manual processes and siloed tools delay patching

31% Decrease in time window for patching before being attacked, over the last two years

54% Say that manual processes put them at a disadvantage when patching vulnerabilities
Security teams respond by trying to hire more resources

64% of healthcare organizations plan to hire additional dedicated resources for patching in the next 12 months.

26% Headcount increase for patching in the next 12 months...or 5.3 people on top of existing staff levels.
But hiring isn’t practical

1.8 MILLION global shortage of cybersecurity professionals by 2022*

33% of cybersecurity jobs don’t receive a single view online**

* Source: Frost & Sullivan, 2017

** Source: Frost & Sullivan, 2017
Processes and siloed tools delay the patching

58%
Say that it is difficult to prioritize what needs to be patched first

9.5 days
Lost coordinating activities across teams for every vulnerability patched

* Source: Frost & Sullivan, 2017
Security’s patching paradox
Hiring more people does not equal better security

- No common view of assets and applications across security and IT
- No easy way to track whether vulnerabilities are being patched
- Things slip through the cracks because emails and spreadsheets are used to manage the patching process

66%
59%
59%

9.5 days

Manual processes and siloed tools delay patching

Time lost coordinating patching across teams
How organizations avoid being breached

Organizations that aren’t breached are better at:

• Detecting vulnerabilities
• Patching vulnerabilities in a timely manner
Broken process can be overcome
Five recommendations for vulnerability response success

1. Take an unbiased inventory of vulnerability response capabilities
2. Tackle low-hanging fruit first, including vulnerability scanning
3. Break down data silos between security and IT
4. Optimize vulnerability response processes, then automate them
5. Retain talent by creating a high-performance culture
A complete approach to responding to vulnerabilities

1. Integrate your vulnerability scanner
2. Automatically prioritize vulnerabilities based on overall risk
3. Automate patch information for IT
4. Coordinate change planning with IT
5. Automation confirms vulnerability resolved
IT wins when IT and security collaborate

- **38%** Drop in maintenance downtime
  - 5% in 5 months
  - 12% Year 1
  - 38% by Year 3

- **40%** Faster service recovery
  - After cyber-attacks

- **50%** Cost savings
  - Tool and service de-dupe

Source: ServiceNow service management with security operations
Q&A

Thank you for joining us

Christopher Killion
Healthcare Solutions Architect
ServiceNow
Download the report

servicenow.com/hc-ponemon

In the last two years, 53% of healthcare organizations have experienced a data breach, and the severity and volume of cyberattacks continue to increase. A global survey of 258 cybersecurity professionals shows that healthcare firms can dramatically reduce the risk of being breached by improving end-to-end vulnerability response processes.
On-demand webinars

Check out our on-demand webinars at www.servicenow.com/events/on-demand-webinars.html
Beginning May 5, the Knowledge 2020 digital experience will showcase all the ways you can unlock productivity through modern digital workflows, highlight the latest customer and platform innovations, and inspire the ServiceNow community to continue to create great experiences for businesses.

Register now – it’s free!