

Information Security Application Design: Improving Signal-to-Noise Ratio

Saurabh Dutta and Ger Joyce

Abstract The clear presentation of critical Information Security insights is a key challenge for Information Security application design. If implemented incorrectly, evidence of a data breach might be lost against the background of unimportant information. Consequently, it is vital for Information Security application design teams to deliver insights, not simply a lot of data, that enables Information Security teams to quickly secure their organization's environments more completely. This paper discusses a Human-Centric approach undertaken to reduce Information Density, and to increase Visual Priority with a view to surfacing key insights quickly within Nexpose, Rapid7's Vulnerability Management application.

Keywords Human factors • Information security • Application design

1 Introduction

In recent times, high-profile Information Security breaches have hit well-known companies, including Sony, JP Morgan, and Home Depot [1]. The increase in Information Security breaches demonstrates how imperative it is for organizations to have a mature Information Security posture [2]. One of the most effective ways for organizations to achieve a mature Information Security posture is to find and remediate the riskiest vulnerabilities within their digital infrastructure. However, Information Security teams, which are generally understaffed, tend to be responsible for tens of thousands of assets. These teams are frequently overwhelmed with

S. Dutta (✉)

Rapid7, 100 Summer St., Boston, MD 02110, USA

e-mail: sdutta@rapid7.com

G. Joyce

School of Computer Science, University of Hertfordshire, Hertfordshire AL10 9AB, Hatfield, UK

e-mail: gerjoyce@outlook.com

© Springer International Publishing Switzerland 2016

D. Nicholson (ed.), *Advances in Human Factors in Cybersecurity*,

Advances in Intelligent Systems and Computing 501,

DOI 10.1007/978-3-319-41932-9_2

the amount of vulnerability information presented to them. They find it difficult knowing where to start, and often focus on the incorrect vulnerabilities or assets.

Yet, providing these key insights has historically been a major challenge for application designers due to the considerable volume of network and user data displayed within an Information Security application User Interface. This is referred to as signal-to-noise ratio [3, 4]. If this ratio is incorrect, insights can easily be lost against the background of inconsequential information. This paper discusses the approach taken at Rapid7, whereby a Human-Centric methodology was applied to solve the problem of providing vital insights to Information Security teams. The improvements to our design of Nexpose Vulnerability Management application using this approach were conducted within an agile environment. This allowed our team to quickly and continuously consider feedback from our customers [5].

2 Approach

Our approach began by better understanding our customers' needs, which is a core element of Human-Centric Design [6], whereby our team conducted multiple rounds of semi-structured interviews. During this phase, customers pointed out that they needed help focusing on the right information ("Give me a plan of action"; "I need guidance"; "Show me what's important").

From the interviews, we defined Proto-Personas [7] to represent customers and their needs. The Proto-Personas were based on the idea of Personas [8], yet were faster to create within fast-paced Agile environments. Modelling customers allowed our team to focus on the right types of customers, and to ensure the correct issues were being addressed [9, 10].

The semi-structured interviews were the start of a Mixed Methods research effort [11], which included Contextual Inquiry, Focus Groups, Surveys (Fig. 1), and Usability Tests. In addition to this effort, our team also measured customers'

Fig. 1 User experience researcher conducting an in-person web-based survey at the Rapid7 UNITED Conference



perception of the usability of Nexpose, Rapid7's Vulnerability Management application. To that end, 42 customers completed the System Usability Scale (SUS) [12], and 11 customers completed 7 Single Ease Questions (SEQ) [13]. While Nexpose scored reasonably well, the results of both the SUS and SEQ quantitative studies revealed how holistic and task-level usability could be improved. Conducting the SUS and SEQ also allowed our team to benchmark where we were before the re-design of Nexpose Vulnerability Management application.

Having gathered our customers' perceptions of Nexpose, as well as their needs, we started the design process to improve the entire User Experience of Nexpose. This resulted in multiple design iterations, where at each stage we gathered feedback from customers. This constant feedback effort included gathering the thoughts of 23 customers in 6 rounds of usability tests, 76 customers with 2 surveys, and 11 customers in a Focus Group/Participatory Design session. All of the information gathered was co-located in a brainstorming room (Fig. 2).

Initial critique from customers on our early designs was invaluable ("I don't necessarily like that"). Subsequent rounds of designs took on a customizable card-based design (Fig. 3), which generated more promising feedback ("This is interesting and has potential"). This indicated that the design team were on the right

Fig. 2 Rapid7 user experience team brainstorming room



track. After several further rounds of interactions and iterations, customers were really enthusiastic about the new design, as well as the ability to focus on key insights (“This interface looks slick”; “Good design and meaningful data”; “It puts a lot of key information up front”).

3 Conclusion

Rapid7 has put our customers at the forefront of our Information Security application re-design effort. The end-result of the Human-Centric approach was an overhaul of Nexpose, Rapid7’s Vulnerability Management application. The previous design (Fig. 4) had primarily been data-driven, as are the majority of Information Security applications in today’s market.

A data-driven design is simply that, the display of data—a lot of data—where it is difficult for Information Security teams to know where to focus. Following the Human-Centric re-design of Rapid7’s Vulnerability Management application, key insights are now far more visible to our customers; enabling our customers to take action quickly which helps to protect their organizations infrastructure from attack (Fig. 5). The re-design effort, therefore, has truly enabled our customers to be more efficient and effective in the management of their organization’s Information Security, even with small, undermanned, overworked teams. Thus, the Human-Centric approach of bringing customers to the forefront of our design effort has allowed Rapid7’s User Experience team to:

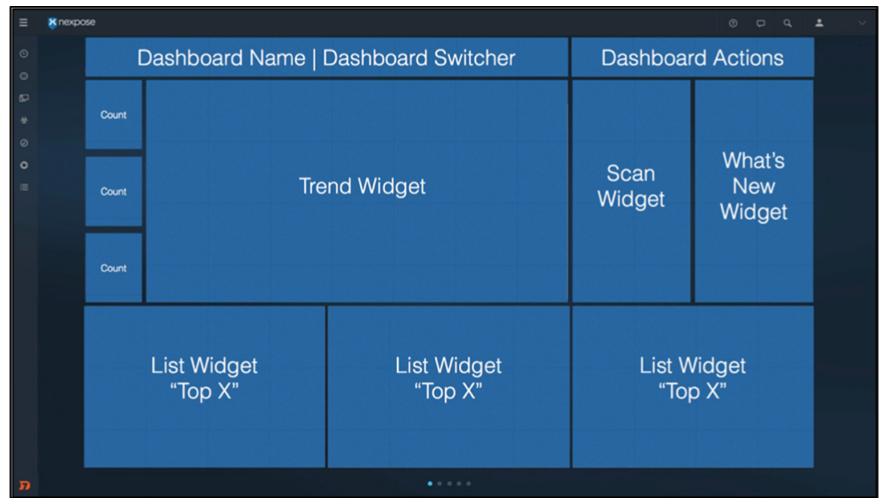


Fig. 3 New Nexpose vulnerability management application dashboard layout

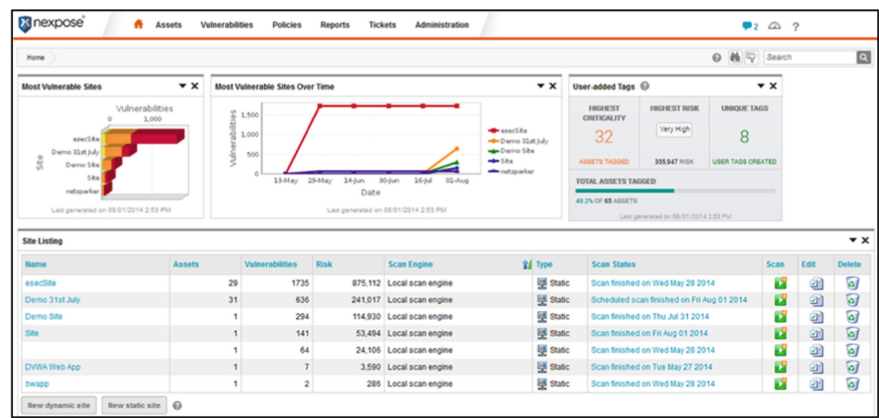


Fig. 4 Original Nexpose vulnerability management application design. This design was primarily data-driven, as is common within information security applications

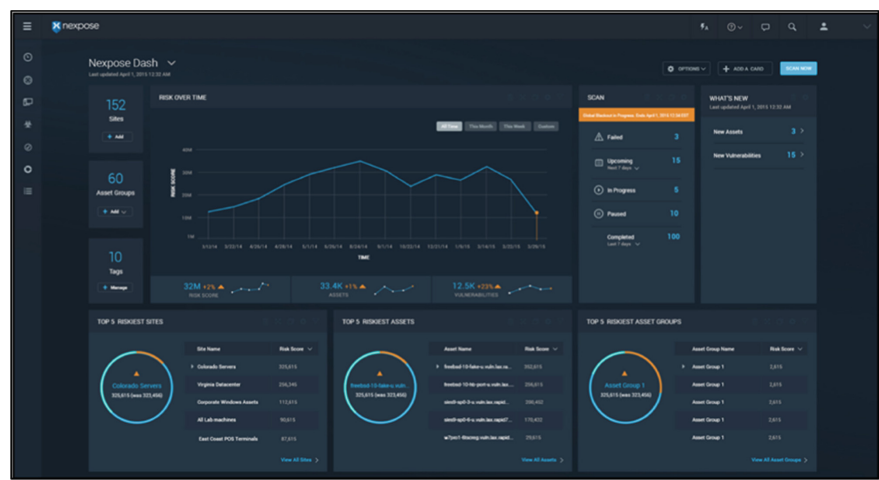


Fig. 5 Final re-designed Nexpose vulnerability management application. The design presents key insights at a glance, allowing information security teams to focus on, and remediate, the riskiest vulnerabilities quickly

- *Reduce Information Density:* The User Interface now only displays important insights, not simply as much data as will fit on the screen, thus balancing the signal-to-noise ratio correctly.
- *Increase Visual Priority:* Critical information is no longer visually identical to less valuable information, so our customers no longer have to work harder to locate the insights they need.

Acknowledgments Rapid7 would like to thank our customers that took time out of their busy schedules to assist the Product Management and User Experience teams during the recent Nexpose Vulnerability Management application re-design effort.

References

1. Tobias, S.: The year in cyberattacks. <http://www.newsweek.com/2014-year-cyber-attacks-295876> (2014)
2. Jang-Jaccard, J., Nepal, S.: A survey of emerging threats in cybersecurity. *J. Comput. Syst. Sci.* **80**(5), 973–993 (2014)
3. Holden, K., Lidwell, W., Butler, J.: Universal principles of design, revised and updated: 125 ways to enhance usability, influence perception, increase appeal, make better design decisions. Rockport Publishers, USA (2010)
4. Tufte, E.R.: Visual display of quantitative information. Graphics Press, USA (1983)
5. Maguire, M.: Using human factors standards to support user experience and agile design. In: *Lecture Notes in Computer Science* (including subseries *Lecture Notes in Artificial Intelligence* and *Lecture Notes in Bioinformatics*), 8009 LNCS, 185–194 (2013)
6. Kim, J.W.: Human computer interaction. Ahn graphics (2012)
7. Gothelf, J., Seiden, J. *Lean UX: Applying lean principles to improve user experience*. O'Reilly Media, Inc, USA (2013)
8. Cooper, A.: *The inmates are running the asylum: why high tech products drive us crazy and how to restore the sanity*. Macmillan, UK (1999)
9. Hourihan, M.: Taking the “You” out of user: my experience using personas. Boxes and Arrows. http://www.boxesandarrows.com/archives/taking_the_you_out_of_user_my_experience_using_personas.php (2004)
10. Negru, S., Buraga S.: Towards a conceptual model for describing the personas methodology. In: *Proceedings of ICCP'12*. IEEE (2012)
11. Creswell, J.W.: *Research design: qualitative, quantitative, and mixed methods approaches*. SAGE Publications, USA (2013)
12. Brooke, J.: SUS-A quick and dirty usability scale. *Usability Eval. Indus.* **189**(194), 4–7 (1996)
13. Sauro, J., Dumas, J.: Comparison of three one-question, post-task usability questionnaires. In: *Proceedings of SIGCHI Conference on Human Factors in Computing Systems*, 1599–1608 (2009)

Advances in Human Factors in Cybersecurity
Proceedings of the AHFE 2016 International
Conference on Human Factors in Cybersecurity, July
27-31, 2016, Walt Disney World®, Florida, USA
Nicholson, D. (Ed.)
2016, XII, 445 p. 108 illus., 65 illus. in color., Softcover
ISBN: 978-3-319-41931-2