SOLARWINDS

Becoming a Prepared CISO

Tim Brown
CISO - SolarWinds

Tim Brown

CISO SolarWinds

Tim Brown serves as Chief Information Security Officer and Vice President of Security for SolarWinds, overseeing internal IT security, product security, and security strategy. Tim has over 20 years of experience developing and implementing security technology.

As a former Dell Fellow and CTO, Tim deeply understands the challenges and aspirations of technology and security professionals. Tim also holds 18 issued patents on security-related topics.

Saturday, December 12 2020
Sunburst

The First Days: Controlled Chaos

- We learned as much as we could as fast as we could and fully committed all our resources.
- Until we determined communication was secure, we coordinated through alternative channels to avoid alerting the unknown threat actors that we had knowledge of the attack.
- We learned of the attack on a Saturday and needed to notify our customers and partners, so we issued an 8-K prior to the stock market opening Monday morning. Within the next 24 hours...
- We knew the threat actors:
    - Were mission-centric, focused, and stealthy
    - Produced well-written and novel code
    - Conducted a well-crafted and sophisticated campaign
    - Attacked our build environment to then attack specific targeted customers
- We had involved the FBI and CISA
- We retained third parties to help with the investigation: DLA Piper, CrowdStrike, and Microsoft.
- We knew this highly sophisticated attack was not in our source code but somewhere in the supply chain.
- We knew three builds were affected, produced between March 2020 and June 2020.
- We knew the *high* end of the number of *potentially* affected customers 18,000 Downloads—but it would be months before the final number was understood under 100

The First Days: Things to know

- It is *beyond* intense.
- Experience is an asset. Engage with experts.
- Time is of the essence — gather information quickly and know that every word and action matters.
- Be sure to have a cross-functional team ready on a moment’s notice.
- A single team cannot manage your response alone — a cross-functional approach is critical from the beginning.
- Be prepared for the road ahead… it’s only the beginning.

The First Days: Culture

- In the first days, we established a collaborative culture with focus
  - Day 1 consisted of virtual war rooms, and by day 2 we moved to physical war rooms in the main office
  - CEO was critical in setting the culture tone.
  - We all had jobs to do, and the team rallied around this direction.
  - The direction and culture stated, "Do your job and help others anyway you can.“
  - Customers as a priority over everything else
  - There was not a 'go it alone' mentality.   We brought in external help, took expert advice, and enlisted third parties to help.
  - Always remember people are going through stages just like the breach and we all internalize situations in different ways.
- What was I feeling?
  - Shock, disbelief, Responsibility – How do I fix this, What will be the outcome , Everyone else in my position is fired
  - Key tenant – Help the customers, Help us move forward

The First Weeks: Getting Organized

- We organized our war room into multiple teams with independent leaders, who met every night. DLA Piper Cyber team was instrumental in approach
  - **IT & Engineering**
  - **Business Escalation and Customer Outreach**
  - **Communications**
  - **Law Enforcement**
- Engaged additional help from Krebs Stamos Group and KPMG Forensics team.
- Communicated what we knew to customers. Built security resource center with FAQs and support materials. Biggest question from customers was “am I affected?”
- Enabled our support teams to manage the load and have the information they needed.

- **“The world is on fire”**
  - Some great research is done, some accurate—and some inaccurate reporting.
  - Highly technical and sophisticated campaigns like this one are difficult for the layperson to understand. This creates a lot of inaccurate and incomplete reporting and narratives, which are then amplified and accelerated by social activity.
  - Because we focused on communicating with our customers, employees, and Partners over controlling a media narrative, the press reached for anyone they can to get quotes, including people who did not have the information and access they claimed they had.
  - The Lawyers quickly appear and start collecting information

The First Weeks: Lessons Learned

- You will be out-numbered, out-marketed, and out-communicated. Misinformation will be everywhere. Don't get sidetracked. Focus on truth in internal and external communications.
- No matter how tough things get, remember the impact on others — especially your customers and employees. The signs are sometimes very subtle.
- Bring in the correct partners. Add partners when necessary. Understand there are many agendas. Be ready for alternative forms of communications and reduced efficiency.
- Create escalation models for each focus area.
- Don't fight the small stuff. If you spend your time responding to every inaccuracy, you take the focus off understanding the why, and how to best support your customers.
- It's OK to not have all the answers. Focus on sharing facts you know to be true. Allow others to focus on attribution.
- Investigations take time. Be aggressive but be patient. Don't miss things, big and small.
- Grow a hard shell this is not going to be easy

The First Weeks: Culture

- The first weeks from a culture perspective…..
  - Clear leadership for each function was established.
  - Trust others were doing their job at an exceptional level
  - This will be one of the hardest and demanding things everyone has gone through
  - People had freedom to act but with oversight and rules…
    - Legal makes legal decisions
    - Marketing/Legal decide the message and who gives it
    - Teams support each other and step in to help in anyway possible
  - Board is also supportive and involved
  - There is tremendous pressure and little sleep. Too much to do and too little time….
  - Everyone in the company stepped up and helped.

- Lessons from a culture perspective…..
  - Establish common objectives and work towards those
  - Put the correct people in the leadership spots
  - Bring them together often and run them like a team
  - Everyone is stressed – Expect lapses
    - Support each other don't expect perfection
  - Keep working there is an incredible amount to get done
  - Bring in experts and expand the team as necessary
  - Leaders need to have emotional maturity always remember what your customers are going through and put them first
- What was I feeling?
  - This happened on my watch
  - Extent of the issue – You just broke the world
  - Out matched, Out numbered
  - Supported, Blamed
  - OK with whatever needed to be done with my position

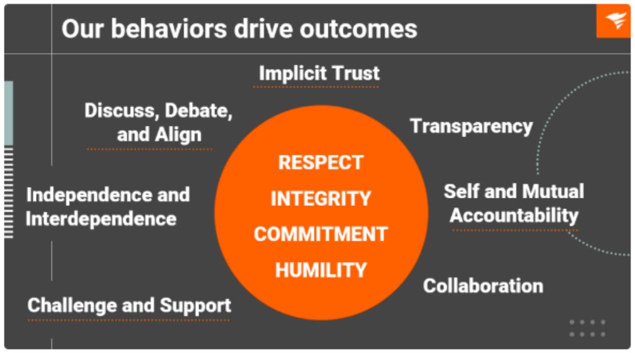
The Months That Followed…

- Investigations continued, with CrowdStrike focused on threat-hunting and KPMG scrubbing the build systems and code repository
- Continued collaborating with FBI and holding briefings, working closely with CISA and the other national defenders
- Found the source for SUNBURST/SUNSPOT and made it available
- Testified before the U.S House and Senate
- Expanded customer meetings to include governments of the world, industry groups, individual customers
- Implemented Orion Assistance Program to help customers
- Revoked our product signing certificate and rebuilt all our products
- Created two-way build environments then next gen build system to validate source matches product
- Finished the investigation in May 2021, and published our RCA

The Months That Followed: Lessons Learned

- Be humble, be honest, and share what you can. Help others learn and iterate.
- Develop a plan to tie everything together and partner with others to reverberate lessons learned throughout the entire experience. Secure by Design
- If you have a cool name, know that it will be used in place of the attackers'.
- Expect additional research to expose additional vulnerabilities and have a response.
- Be prepared for hard questions.
- Use it as an opportunity to become exemplary.
- Continue sharing with the community in the aftermath.

SolarWinds Culture Code and Values



Our behaviors drive outcomes

Implicit Trust

Discuss, Debate, and Align

Transparency

Independence and Interdependence

RESPECT
INTEGRITY
COMMITMENT
HUMILITY

Self and Mutual Accountability

Collaboration

Challenge and Support

SolarWinds Culture Code

At SolarWinds, we believe behaviors drive outcomes. Our Culture Code highlights behaviors we desire to incorporate and proliferate across all Solarians and their extended teams. Our CARE values empower us to delight our customers, build trust, and win as a team. Our Culture Code surrounds four RICH behaviors: **Respect**, **Integrity**, **Commitment**, and **Humility**.

It is our fervent hope that Solarians should understand, demonstrate, celebrate, and enrich these values and behaviors, upholding them in all we do and decide.

Our Values

- Collaborative – We work together with everyone to deliver customer success in an environment where we challenge and support each other while also recognizing and celebrating individual successes and team accomplishments.
- Accountable – We hold ourselves and others accountable to uphold and continually improve our standards of behavior and outcome orientation.
- Ready – We strive to learn and improve from every engagement and situation. We adapt to address planned and unplanned needs.
- Empathetic – We strive to appreciate different perspectives, walk in others' shoes, and seek to understand before rushing to judge.

Our Values

C A R E

Collaborative | Accountable | Ready | Empathetic

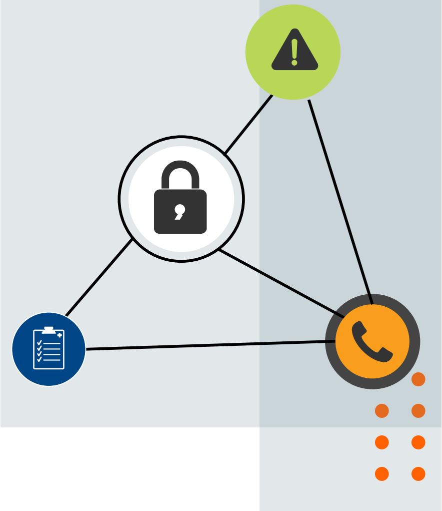
The Months that Followed: Culture

- The next Months from a culture perspective…..
  - Secure by Design theme is introduced across the company
  - Culture Code and Values defined with new leadership
  - The next months the work starts getting done and pressure is on to make progress
  - Leadership and Trust allows an incredible amount to get done
  - A shift from panic and incredibly intense to steady state intensity and difficult schedules
  - The backlog get's cleaned up now recovery is in full swing
  - Keeping the culture focused and working under one theme focuses the company
  - Expect set backs and changes.   Embrace change and prepare.

- Lessons from a culture perspective…..
  - Understand the intensity of the weeks will start to wane as you go into months
  - Continue to re-inforce the reason for all the work and the direction that is being taken
  - Re-inforce the culture and values of the company
  - CARE Values – Make them real establish them as part of reviews
- What was I feeling?
  - I'm keeping my job
  - How do I help not just our customers but the industry
  - Be transparent share as much as possible with as many as possible
  - Appreciation from unlikely sources

The Years That Followed…

- Continue on the path of sharing and transparency
- Starting correcting inaccuracies in press/media
- Reach as many customers, partners, vendors and communities as possible
- Show exemplary actions externally and internally
- Continue to invest in Secure by Design with people, technology and partners
- Embrace efforts to improve overall software design and transparency



Results

  - Renewal Rates are over 95% and the company is very healthy
  - Would not have happened if the customers did not love the products

The Years That Followed: Lessons learned

- Be patient this takes time
- Use the event as a catalyst for good
    - Executive Order
    - Cyber security Strategy
    - Attestation for Software Providers
- Be prepared for potential legal actions that will test individuals and the company
- Use events to elevate the CISO position and develop communities
- Continue with the umbrella program “Secure by Design”
- Be not just good but exemplary in sharing and in technology

The Years that Followed: Culture

- The Years from a culture perspective…..
  - Patience is the key. You will be tested
  - Do everything possible to create alignment
  - Everyone wants to move forward but external factors are out of your control
  - Continue to reinforce a strong culture
  - Support the process and look for good to come from difficult situations
  - Trust in the process
  - Align with great external teams and get back to protecting the company and the customers

- Lessons from a culture perspective…..
  - Be patient no matter how long it takes
  - Look for good to occur from your experience
  - Culture extends beyond companies into communities, partners and customers
  - Share experiences and lessons with others
  - Help the community and the world get better
  - Focus on the good and helping others
- The CISO state of mind
  - Focus on the work of protecting the company
  - The legal issues provided another opportunity to help
    - Raising awareness of the legal issues that can arise
    - Build understanding and need for alignment/coverage
  - Keep moving forward as an example for the industry
  - Dec 12, 2020, October 2022 initial Wells, Sept 2023 SEC Charges, July 2024 Judge dismisses most claims, Next stages in process

Looking back

- What I wish I had
  - Past experience of a major incident
  - More testing and simulation and scenario planning
  - We had good relationships, but they could have been stronger internal and external
  - More knowledge and expectation of the legal process
  - I wish I knew then what I know now
- What has kept me going
  - The support of the company, the employees and it's leadership
  - The community support from CISOs, Industry groups, and so many individuals
  - The good that has come of our situations
    - More attention to security
    - More support for the CISO
    - Stronger communities, more sharing, more transparency
    - Stronger and more resilient companies across the globe

THANK YOU

This presentation contains forward-looking statements regarding future product plans and development efforts. SolarWinds considers various features and functionality prior to any final generally available release. Information in this presentation regarding future features and functionality is not and should not be interpreted as a commitment from SolarWinds that it will deliver any specific feature or functionality in the future or, if it delivers such feature or functionality, any time frame when that feature or functionality will be delivered. All information is based upon current product interests, and product plans and priorities can change at any time. SolarWinds undertakes no obligation to update any forward-looking statements regarding future product plans and development efforts if product plans or priorities change.